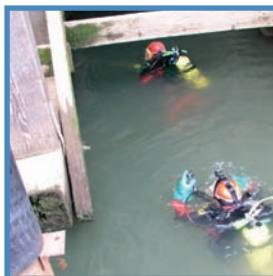
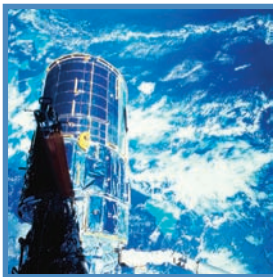


port security requirements

Industrial Opportunities for Small and Medium Enterprises



A Report prepared by
CFN CONSULTANTS  **CFN Consultants**
A Partnership

December 2004

sponsored by



 Western Economic Diversification Canada Diversification de l'économie de l'Ouest Canada



Contents

Executive Summary	5
Sommaire	7
Introduction.....	9
Statement of Objective.....	11
The National Security Environment	11
Broad Government Announcements And Allocation of Resources	11
Public Safety and Emergency Preparedness Canada	14
National Security Policy	16
Departmental Responsibilities	19
The Maritime Security Environment	21
Evolution of Departmental Cooperation.....	21
An Assessment of Port Security	25
Port Security Requirements	25
Responsibility Interfaces.....	26
Security Assessments-Considerations for the Port Security Regime	27
Requirements for Port Security.....	29
Intelligence.....	30
Surveillance and Monitoring (Collecting Information)	30
Collating Information.....	31
Disseminating Information	32
Response Capability.....	33
An Integrated Port Security Model.....	33
A Generic Description of a Layered Integrated Port Security Regime	34
Scaling the Model for Regional, Local and Occasional-Use Ports and Marine Facilities	39
Analysis of East and West Coast Industrial Ability to Meet the Model.....	40
Conclusions.....	41
Summary of Industrial Opportunities	43
Follow On Work	45
Glossary of Acronyms	46
Annex A – Database of East and West Coast SMEs	47
Annex B – Potential Investigation Areas for SMEs	49
Annexe B – Domaines d’exploration potentiels pour les PME	51

Executive Summary

Prior to 11 September 2001, the Western nations, and Canada in particular, perceived security issues as: criminal activity, appropriately countered through industrial security precautions and law enforcement functions, and military threats addressed through the domain of national defence. This simplistic and discrete consideration has evolved into a more realistic and comprehensive approach to national security in which there is a recognized, continuous spectrum of risk to good order, from low-grade pilfering to international hostilities, with terrorism, illegal immigration, smuggling and general commercial disruption all contained therein.

In response to this new perception of national security, the Government of Canada has made several commitments to fund new security initiatives, issued the first National Security Policy and re-organised departmental responsibilities to address the new security environment. The Department of Public Safety and Emergency Preparedness was formed to coordinate overall government monitoring and response. Transport Canada has retained responsibility for maritime security policy. A foundation for the marine security policy is the International Ship and Port Facility Security (ISPS) Code, accommodated in Canada as the Maritime Transportation Security Regulations, promulgated under the Marine Transportation Security Act.

The economic well-being of our regional ports depends upon transshipment to the United States of America (USA). To retain this business and to demonstrate due diligence in the case of a potential disaster, the security of Canada's regional ports must be maintained to the highest possible standard. It is also clear that the regulatory framework will continue to become more rigorous over time. Equally to retain the lucrative cruise ship business, the security of all terminals that share in this enterprise must also be guaranteed.

The objective of this paper is to identify industrial opportunities for small and medium enterprises emerging from the new port security environment. The authors have taken a broad view of port security to include monitoring and response capability in the marine approaches to Canada. Port security to be effective begins when a vessel leaves its previous port of call.

To ensure a complete understanding of marine and port security issues, this report includes a summary of important government decisions in defining the maritime security goals, an examination of the basic tenets of effective security measures and a proposal for an integrated marine security model. The model is used as the vehicle for revealing areas of current industrial activity and exploring potential areas that warrant research and development initiative.

The conclusion of this paper demonstrates that there are many significant opportunities for small and medium enterprises, and it is suggested that technology demonstrators are a useful mechanism for addressing security requirements and supporting the development

of new technologies and services as well as showcasing them for export potential. These opportunities cover every category of enterprise from sensors and detectors, information management, security services, training, communications and the integration of many of these individual components into a security system.

Sommaire

Avant les événements du 11 septembre 2001, les nations occidentales, et particulièrement le Canada, percevaient les questions de sécurité sous deux angles : celui de l'activité criminelle, que l'on peut contrer au moyen des mesures de sécurité industrielle et les services d'application de la loi, et celui de la menace militaire, qui relève du domaine de la défense nationale. Cette perception simpliste et distincte a évolué pour aboutir à une démarche de sécurité nationale plus réaliste et globale où l'on tient compte d'un éventail permanent de menaces au bon ordre, allant du simple vol aux conflits internationaux, sans oublier le terrorisme, l'immigration illégale, la contrebande et la perturbation du commerce.

En réaction à cette nouvelle perception du contexte de la sécurité nationale, le gouvernement du Canada a pris plusieurs engagements pour le financement de nouvelles initiatives de sécurité, publié la première politique de sécurité nationale et restructuré les responsabilités ministérielles en fonction de ce nouveau contexte de la sécurité. Le gouvernement a formé le ministère de la Sécurité publique et de la Protection civile pour coordonner la démarche globale de surveillance et d'intervention du gouvernement. Transports Canada a conservé la responsabilité de la politique de sécurité maritime. L'un des fondements de cette politique de sécurité maritime est le Code international pour la sûreté des navires et des installations portuaires (ISPS), mis en œuvre par l'entremise du *Règlement sur la sûreté du transport maritime* adopté en vertu de la *Loi sur la sûreté du transport maritime*.

Il est également évident que la vitalité économique de nos ports régionaux repose sur le transbordement vers les États-Unis. Pour maintenir ce commerce et démontrer la diligence voulue dans l'éventualité d'un désastre, il faut maintenir le plus haut degré possible de sécurité dans les ports régionaux du Canada. Il est également manifeste que le cadre réglementaire deviendra plus rigide au fil du temps. De même, pour préserver le lucratif marché des navires de croisière, il faudra également garantir la sécurité de tous les terminaux portuaires qui soutiennent cette industrie.

Ce document est publié dans le but d'identifier les débouchés industriels qui s'offrent à la petite et moyenne entreprise dans ce nouveau contexte de la sécurité portuaire. Les auteurs ont abordé la sécurité portuaire dans le sens large, allant de la surveillance à l'intervention dans les eaux limitrophes du Canada. En d'autres termes, si la sécurité portuaire ne débute qu'à l'entrée du port, il est déjà trop tard.

Pour permettre au lecteur de bien saisir le dossier de la sécurité maritime et portuaire, le rapport comprend un sommaire des décisions importantes que le gouvernement a prises en définissant les objectifs de sécurité maritime, un examen des principes de base qui sous-tendent l'efficacité des mesures de sécurité et un projet de modèle de sécurité maritime intégré. Le modèle sert d'instrument pour révéler les domaines d'activité actuels et explorer les secteurs d'intérêt pour la recherche et le développement.

La conclusion montre qu'il existe de nombreux et importants débouchés pour la petite et moyenne entreprise, et laisse entendre que les démonstrateurs de technologie sont des mécanismes utiles pour répondre aux besoins de sécurité et soutenir le développement de nouveaux produits et services, de même que pour les exposer en vue d'exploiter leur potentiel d'exportation. Les débouchés recourent tout l'éventail des domaines d'entreprise, allant des capteurs et détecteurs à la gestion de l'information, en passant par les services de sécurité, la formation, les communications et l'intégration de ces diverses composantes dans les systèmes de sécurité.

An Analysis of Industrial Opportunities for Small and Medium Enterprises in Port Security Requirements

Introduction

1. The terrorist acts perpetrated on 11 September 2001 marked a watershed in the appreciation of national security issues. In general, until that time, the Western nations, and Canada in particular, perceived security issues in two ways: criminal activity, appropriately countered through industrial security precautions and law enforcement functions, and military threats addressed through the domain of national defence. This simplistic and discrete consideration has evolved into a more realistic and comprehensive approach to national security in which there is a recognized, continuous spectrum of risk to good order, from low-grade pilfering to international hostilities, with terrorism, illegal immigration, smuggling and general commercial disruption all contained therein. The Homeland Defence initiatives in the United States of America (USA) and the establishment of a portfolio for public safety and emergency preparedness in Canada arise directly from this recognition of the modern national security environment.

2. Within the larger rubric of national security, there are a number of subsets within subsets, and some areas of interest are more evolved than others. The Interdepartmental Marine Security Working Group (IMSWG¹), which was established in October 2001 by Transport Canada (TC)², continues to function as the centrepiece for the coordination of Canada's marine security activities. Transport Canada chairs the group, which now comprises 17 federal departments and agencies. The role of the IMSWG is to co-ordinate federal response to marine security, analyze our marine system for security gaps and develop possible mitigation initiatives to address these gaps. These inter-relationships are complex and impinge on many legislative and regulatory regimes. However, within the greater maritime security envelope, there are specific requirements that have emerged concerning ship and port security.

3. Following a week-long diplomatic conference held at the London headquarters of the International Maritime Organization (IMO) from 9-13 December 2002, a number of amendments to the 1974 Safety of Life at Sea Convention (SOLAS) were adopted. The most far-reaching of these amendments is the International Ship and Port Facility Security (ISPS) Code. The ISPS Code — which came into effect on 1 July 2004 — is a new, comprehensive security regime that seeks to establish an international framework of co-operation between governments, government agencies and the shipping and port

¹ The use of acronyms is common in Government, particularly in the security and defence areas. They are useful to avoid tedious repetition of common phrases and for the sake of brevity. For the convenience of readers, each acronym in this report is defined in the text the first time it is used, and a glossary of all acronyms used in this report is included on page 42.

² http://www.tc.gc.ca/vigilance/sep/marine_security/enhancing/initiatives.htm

industries in order to detect and take preventive measures against security incidents affecting ships or port facilities used in international trade.³

4. In January 2003, the Government of Canada announced a \$172.5 million, five-year package of initiatives to further enhance security of Canada's marine transportation system and maritime borders. The main security projects in this package focus on safeguarding and protecting marine infrastructure, providing surveillance of Canadian waters and improving emergency response capabilities. Specific projects include:

- increased surveillance and tracking of marine traffic, including "near-real-time" identification and tracking of vessels in Canadian waters;
- screening of passengers and crew on board vessels;
- installing new detection equipment in port to screen containers for radiation; and
- developing and implementing new security requirements in line with recent recommendations of the International Maritime Organisation (i.e., ISPS Code).

5. On 12 December 2003, the Government of Canada announced the creation of a new portfolio for public safety and emergency preparedness. It includes emergency preparedness, crisis management, national security, corrections, policing, oversight, crime prevention and border functions. Clearly, as a complement to other departmental mandates, such as Transport Canada, this new portfolio will assume overall responsibility for security issues. However, it is not yet clear what the new organization will look like, where money will be assigned to projects and what role Canadian industry will play in satisfying the Government's security requirements. In the area of port security, this is perhaps better defined than elsewhere due to the recent implementation of the ISPS Code. The Canadian regulations pertaining to the ISPS Code are included in the Maritime Transportation Security Regulations, promulgated under the Marine Transportation Security Act and published in the Canada Gazette Part II, Vol 138, No 11 (2004-06-02).

6. In addition to the legal obligation to satisfy the minimum requirements of the ISPS Code as spelled out in the regulations, there is an economic incentive to promote the reputation of Canadian port facilities as safe and secure portals into and out of North America. In the commercial world, where perception has as great an effect on the preferred routes for the movement of cargo as physical reality, there are competitive reasons for establishing a highly visible port security profile. As an indicator, the Port of Baltimore, for example, has made less than subtle inferences that cargo destined for the mid-West of the USA would be handled more safely and expeditiously through the Maryland facilities than relying on "foreign" routes. Were this to become a prevailing sentiment in the USA, potential economic impact on Canadian ports does not require elucidation.

7. As a consequence of this important new emphasis on port security, there are clearly industrial opportunities to be realised in addressing Government and commercial requirements. Most large corporations have mature business development processes that

³ http://www.tc.gc.ca/vigilance/sep/marine_security/isps/menu.htm

permit them to track and appreciate these opportunities. However, there is much potential work to be done in the security arena by small and medium enterprises that lack the sophisticated means to find and evaluate opportunities. Particularly, as they have proven to be the engine for employment and growth in the Canadian economy, it would be of value to provide a summary of security developments and conduct an analysis of the industrial opportunities for small and medium enterprises in port security requirements.

Statement of Objective

8. The objective of this report is to provide the Maritime Awards Society of Canada with an analysis of opportunities for small and medium enterprises (SMEs) in port security requirements and identify the areas where further development is necessary.

The National Security Environment

Broad Government Announcements and Allocation of Resources

9. From the immediate aftermath of the September 2001 attacks on the USA right up to the most recent national election, the Federal Government has made significant commitments to fund new security initiatives. While these have been well-publicised, it is useful to include a summary of the various announcements in this report. While many of these announcements do not directly address port security, it is only one aspect of the larger security mosaic where the other areas contribute to the environment in which port security can be effectively maintained.

- October 2001 – New RCMP Funding Initiatives - \$59M
 - Enhance analytical intelligence sharing and operational technology;
 - Support protective operations;
 - Enhance security activities at airports
 - Enhance security activities at ports and border crossings;
 - Enhance security activities at major centres; and
 - Enhance staffing requirements for priority areas

(Note: The RCMP funding increment was increased to \$576M in the December 2001 Federal Budget)

- December 2001 – Budget 2001 Major Security Funding Thrusts
 - Intelligence and Policing (including Oct 01 RCMP Allocation) - \$1.6B
 - Equipping and deploying more intelligence and police officers - \$1.18B
 - Improving coordination and information sharing - \$76M
 - Enhanced marine security - \$60M

- Cutting off terrorist financing - \$63M
- Other initiatives - \$163M
- Contingency - \$95M
- Emergency Preparedness and Support for Military - \$1.6B over five years
 - Expanded anti-terrorist capacity (JTF 2) - \$119M
 - Nuclear, Biological, Chemical and Radiological threats - \$513M
 - Operation Apollo (War on Terrorism) - \$210M
 - Capital procurement (on-going projects) - \$300M
 - Emergency Preparedness - \$396M
 - Contingency - \$100M
- Border Security and Facilitation - \$646M over five years
 - Expediting pre-approved travellers - \$58M
 - Better tools for risk assessment and detection - \$67M
 - Better equipment for detecting explosives, firearms and other dangerous shipments - \$107M
 - New secure internet-based technology re: small business compliance - \$14M
 - Integrated Border Enforcement Teams - \$135M
 - Other initiatives - \$226M
 - Contingency - \$40M
- Border Infrastructure - \$600M over five years
 - To support and amplify the benefits of the Canada-US NEXUS border-wide “fast-lane” program and the Free and Secure Trade (FAST) program
 - QEW improvements in Niagara
 - Highway improvements in Saskatchewan - \$5M
 - Canada-BC investment at Lower Mainland crossings - \$211M
 - 5-year shared Canada-Ontario investment at the Windsor gateway - \$300M
 - shared Canada-Ontario investment for major road arteries and border crossing enhancements - \$325M
- Air Security - \$2.2B over five years
 - Enhanced pre-board screening of passengers - \$128M/year
 - Acquisition, deployment and maintenance of new state-of-the-art explosives detection equipment at airports
 - Certification and testing of security officers responsible for screening services
 - Program for secure cockpit doors - \$35M
 - Federal contributions for security-related airport policing - \$20M
 - Contracting for armed police on board aircraft
 - Protection of ports and critical infrastructure - \$60M
 - Airport security data fusion
 - Strategic highway infrastructure program
- Screening Entrants to Canada - \$1B over five years

- Fraud resistant documents - \$287M
 - Resources for refugee detention, removal and determination - \$210M
 - Other technologies to enhance more accurate and faster screening - \$395M
 - Contingency - \$110M
- January 2003 – Transport Canada 5-year Funding Allocation
 - Enhanced Marine Transportation and Maritime Border Security Initiatives - \$172M
 - Increasing surveillance and tracking of marine traffic, including “near-real-time” identification and tracking of vessels in Canadian waters⁴
 - Screening of passengers and crews on board vessels
 - Installing new detection equipment in ports to screen containers for radiation
 - New funding for the enhancement of the RCMP Emergency Response Teams and the establishment of permanent investigators at major ports
 - Enhancing collaboration and coordination among Government departments and agencies
 - Making further improvements to port security by establishing restricted areas and requiring people working within these areas to undergo thorough background checks
 - Developing and implementing new security requirements in line with recent recommendations of the International Maritime Organisation (ISPS)
- February 2003 – Federal Budget
 - Incremental increase to security reserve - \$75M
 - Operation Apollo incremental increase - \$270M
- December 2003 – DND Strategic Investment Capability Plan (Funding under Public Security and Anti-terrorism)
 - High Frequency Surface Wave Radar - \$43M
 - Counter-terrorism and special operations enhancement - \$40M
- March 2004 – Federal Budget
 - Additional Defence spending for international commitments – \$300M
 - Additional funding over five years for security contingency reserve - \$605M
- April 2004 - Public Safety and Emergency Preparedness – National Security Policy - \$690M
 - Enhancing intelligence capabilities - \$137M
 - Securing critical government information systems - \$85M
 - Real-time identification project (fingerprints) – \$100M
 - Passport security strategy - \$10.3M
 - Integrated Threat Assessment Centre - \$30M

⁴ High Frequency Surface Wave Radar, see December 2003, is a component of this increased surveillance

- Government Operations Centre - \$15M
- Marine Security - \$308M
 - Maritime Security Operations Centres - \$165M
 - Enhanced communications between Canadian Forces, RCMP and CCG vessels, aircraft and operations centres⁵ - \$38M
 - Enhanced port security (*when requirements identified*) - \$100M
- May 2004 – Enhancement of Port Security - \$115M
 - The federal contribution covers 75% of funding required for procurement of new surveillance equipment, improving security fences and improving communications equipment. This part of the \$605M security contingency reserve was announced in the March 2004 Federal Budget.

10. Although there have been many announcements made regarding commitments to security issues, there is not an easily accessible summary of how these funds are actually being assigned to projects and the status of the projects in the government procurement cycle. As of mid-October 2004, verbal queries to Public Safety and Emergency Preparedness Canada, the newly formed Government portfolio with overall coordination responsibilities for security, the Department of Finance and the Treasury Board were not able to provide any publicly available information regarding the current status of expenditure in this field. This is clearly an area that requires additional effort to map commitments against industrial opportunities.

Public Safety and Emergency Preparedness Canada

11. On 12 December 2003, the Prime Minister announced the creation of a new Government portfolio: Public Safety and Emergency Preparedness Canada (PSEPC). It includes emergency preparedness, crisis management, national security, corrections, policing, oversight, crime prevention and border functions.

12. According to PSEPC's, the establishment of this new portfolio "created a new Minister of Public Safety and Emergency Preparedness to integrate into a single organization the core activities of the previous Solicitor General portfolio that secure the safety of Canadians and other activities required to protect against and respond to natural disasters and security emergencies. Additionally, it integrated the Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) (formerly under the Minister of National Defence) to maximise emergency preparedness and responses to natural disaster and security emergencies, as well as improving connections to provincial and territorial emergency preparedness networks, and by adding the National Crime Prevention Centre to actively support crime prevention. It also created a Canada Border

⁵ The enhanced communications is an IMC3 initiative to provide an information distribution system that supports planning and the execution of maritime operations, by providing a domestic maritime situational awareness system to Department of National Defence (DND) Kingston-class ships, and sea-going vessels operated by the Canadian Coast Guard (CCG). In particular, the objective of IMC3 is to create a deployable interagency tool to enhance situational awareness to improve informed decision-making and facilitate coordinated action.

Services Agency (CBSA) to build on the Smart Border Initiative and the important progress that has been made in expediting trade and travel, while enhancing security with respect to high risk arrivals, and to continue to work in close collaboration with business, labour, immigrant and refugee groups, and other important stakeholders in pursuing these changes.”

13. It is apparent that the new portfolio will have broad responsibilities, as it now consists of five branches: Emergency Management and National Security (composed of the former OCIPEP and the National Security Directorate, responsible for operational readiness and response, including the Government of Canada Operations Centre; policy and program coordination; critical infrastructure protection and emergency management programs; and national security); Policing and Law Enforcement (composed of the pre-existing Enforcement and Organised Crime Directorate, Policing Policy Directorate and Integrated Justice Information, responsible for policing, borders, firearms policies and integrated justice information functions); Community Safety and Partnerships (composed of the National Crime Prevention Centre, Corrections Policy Directorate, and the Aboriginal Policing Directorate, responsible for crime prevention, corrections and conditional release and aboriginal policing); Portfolio Relations and Public Affairs (responsible for communications, strategic policy, ministerial coordination and liaison and the transition secretariat); Corporate Management (responsible for comptrollership, office of the chief information officer, management assurance and human resources); and General Counsel and Inspector General (directly reporting to the Deputy Minister).

14. In addition to the branches of the portfolio, the Minister is responsible for six agencies, including the Royal Canadian Mounted Police (RCMP), the Canadian Security and Intelligence Service (CSIS), the Correctional Service of Canada, the National Parole Board, the Canadian Firearms Centre and the CBSA. The Minister’s span of control will extend over some 55,000 employees and operate on a budget of approximately \$7B annually.

15. Until mid-October 2004, officials assigned to this portfolio were still dealing with basic organizational issues, including the drafting of legislation, which was tabled in the House of Commons 8 October 2004, to create PSEPC as a Department of the Federal Government. Consequently, until the legislation is enacted, the fulfillment of the Minister’s responsibilities is being executed under the legislative mandates of the constituent departments and agencies that have been amalgamated as PSEPC. One of the salient questions arising from the new legislation will be the degree to which this Department will exercise direction over the other departments with responsibilities in the security domain. Hence, it is not yet clear how this department will play in the domain of Maritime and Port Security. At the present time, as discussed below, it is TC that has the extant leadership position in this critical area.

National Security Policy

16. In an effort to put substance behind the broad commitments for funding and the organization of PSEPC, the Prime Minister introduced *Securing an Open Society: Canada's National Security Policy*, in April 2004. The National Security Policy (NSP) was identified as the first comprehensive and integrated national security policy in Canada's history. The NSP focuses on addressing three core national security interests:

1. Protecting Canada and Canadians at home and abroad;
2. Ensuring Canada is not a base for threats to our allies; and
3. Contributing to international security.

17. It contains several measures to help build a more integrated security system in a way that is consistent with the goals of the policy:

- An Integrated Threat Assessment Centre will be established to ensure that all threat-related information is brought together, assessed and reaches all who need it in a timely and effective manner.
- The Government will establish a National Security Advisory Council, which will be made up of security experts external to government.
- An advisory Cross-Cultural Roundtable on Security, composed of members of Canada's ethno-cultural and religious communities, will be created.
- The new Department of Public Safety and Emergency Preparedness will be designated as the body responsible for the testing and auditing of federal departments' key security responsibilities and activities.

18. The NSP also includes chapters on six key strategic areas. Each chapter builds on important steps already taken, addresses specific security gaps, and sets out the principles upon which the policy will be implemented and evolve. Several specific new measures have spending implications. New investments in these measures total \$690 million and will be funded from the security contingency reserves in Budget 2001 and Budget 2003, and most recently supplemented by Budget 2004. As taken from the Executive Summary of the policy document, highlights of key measures include:

- *Intelligence*
 - *Further investments will be made to enhance Canada's intelligence collection capacity, with a focus on Security Intelligence.*
 - *An arm's-length review mechanism for RCMP national security activities will be created.*
 - *The proposal to establish a National Security Committee of Parliamentarians will be implemented.*
- *Emergency Planning and Management*
 - *A new Government of Canada Operations Centre will provide stable, round-the-clock co-ordination and support across government and to key national players in the event of national emergencies.*

- *The Emergency Preparedness Act will be reviewed and modernized to achieve a seamless national emergency management system.*
- *A permanent federal-provincial-territorial forum on emergencies is proposed.*
- *The Government is committed to co-locate, where practical, with provincial, territorial and municipal emergency measures operation centres.*
- *The Government will release a position paper this summer setting out the key elements of a proposed Critical Infrastructure Protection Strategy for Canada.⁶*
- *The Government will increase its capacity to predict and prevent cyber-security attacks against its networks.*
- *A national task force, with public and private representation, will be established to develop a National Cybersecurity Strategy.*
- *Public Health*
 - *The new Public Health Agency of Canada and the position of a Chief Public Health Officer for Canada will be created.*
 - *The National Microbiology Laboratory in Winnipeg and the Laboratory for Foodborne Zoonoses in Guelph will be enhanced.*
 - *The National Emergency Services Stockpile System will be replenished and updated.*
 - *The Government will establish Health Emergency Response Teams made up of health professionals across the country to enhance capacity to respond to health emergencies.*
 - *The Government continues its commitment to work with the provinces and territories to address vulnerabilities and build on existing public health strengths across Canada.*
 - *The Government will increase public health surveillance capacity across the country.*
- *Transport Security*
 - *The Government is strengthening marine security through the implementation of a six-point plan that will:*
 - *clarify responsibilities and strengthen co-ordination of marine security efforts;*
 - *establish networked marine security operations centres;*
 - *increase the Canadian Forces, RCMP, and Canadian Coast Guard on-water presence and Department of Fisheries and Oceans aerial surveillance;*
 - *enhance secure fleet communications;*
 - *pursue greater marine security co-operation with the USA; and*
 - *strengthen the security of marine facilities.*
 - *In partnership with the private sector and our international partners, Canada will identify strategies to enhance our aviation security, including air cargo.*

⁶ A position Paper on a National Strategy for Critical Infrastructure Protection was issued on 12 November 2004

- *The Government will improve and extend security background check requirements for transportation workers.*
- *Border Security*
 - *Canada will deploy facial recognition biometric technology on the Canadian passport, in accordance with international standards.*
 - *The Government will complete implementation of the RCMP Real Time Identification Project to achieve an automated and modern fingerprint system.*
 - *The Government will table new measures to streamline our refugee determination process to ensure efficient protection for people genuinely in need and to facilitate effective removals of people attempting to abuse our refugee program.*
 - *Canada is developing a next-generation smart borders agenda with Mexico and the USA, building on the success of the Smart Borders Declaration signed with the USA in December 2001.*
 - *Working with our international partners and in international forums, such as the G8 and the World Customs Organization, Canada will internationalize the Smart Borders model.*
- *International Security*
 - *The Government will make Canada's national security one of the top priorities in its International Policy Review.*
 - *The Government is committed to ensuring that the Canadian Forces are flexible, responsive and combat-capable for a wide range of operations, and are able to work with our allies.*
 - *Beginning with the establishment of a dedicated capacity-building fund, Canada will leverage its experience in building peace, order and good government to help developing, failed and failing states.*
 - *Canada will continue to play an important role in countering international terrorism, preventing the proliferation of weapons of mass destruction, and defusing key intra- and interstate conflicts.*

19. While, the provisions for transport security are most germane to this study, it is clear that the rest of the policy is important to defining the context in which the marine and port security requirements reside. However, the single key element SMEs will likely want to investigate in the short-term is the provision for enhancing port security. The Federal Government has committed \$115M over fiscal years 04/05 to 07/08 on a cost-share basis, in which they will provide up to 75% of costs, to assist all Canada's ports and terminal operators with the cost of strengthening their security systems and programs. This application-based program is limited to expenses incurred after April 2004 for the purposes of meeting compliance with ISPS Code and the Canadian regulations. It is anticipated that the guidelines and information package for application to TC will be distributed to ports and marine facilities with approved security plans before the end of October 2004.⁷

⁷ The Marine Security Contribution Program was announced on 2 Dec 2004

Departmental Responsibilities

20. Notwithstanding the overarching responsibility of PSEPC, it is important to understand the direct responsibilities of the other Government departments, because, in most cases, the funds assigned for security projects will be delegated to specific departments for implementation.

21. Roles of the Government departments and agencies under the NSP and as they relate to marine and port security are as follows:

- TC is responsible for the co-ordination of Canada's marine security activities through its own mandate as well as the chairing of IMSWG. As such it provides horizontal coordination between the departments involved and takes the lead in seeking Cabinet approval for the expenditure of funds on security related projects. TC is responsible for marine security policy and developing the regulatory frame work under which it is applied. Although TC has a role in the operational enforcement and response to violations of the regulations, operations are not a prime responsibility of the Department. The TC national situation centre (SITCEN) processes "96 Hour Reports" (notification of a vessel's arrival in Canadian waters) and disseminates appropriate information to other Government departments with marine security enforcement responsibilities. The department's inspectors monitor and enforce the security regulations that it has issued to comply with the ISPS Code. In addition, TC maintains close ties with its regulatory counterparts internationally, particularly those in the USA
- The Canadian Forces (CF) mission is to defend Canada and contribute to international peace and security.⁸ Under Canadian defence policy, the CF are called upon to fill three major roles: protecting Canada, defending North America in co-operation with the USA, and contributing to peace and international security. As described earlier, within Canadian territory and the exclusive economic zone, the CF can enforce Canadian law only when tasked to do so, otherwise the enforcement function is exercised by those with the appropriate jurisdictional authority, specifically RCMP or Department of Fisheries and Oceans (DFO) or, now, CBSA officers embarked in a naval vessel for that purpose. With respect to the new initiatives in maritime security, the CF is tasked with creating and organising the Marine Security Operations Centres (MSOCs) as identified in the NSP, developing the Marine Information Management Data Exchange (MIMDEX) identified by IMSWG

⁸ Under the provisions of the *National Defence Act*, the Canadian Forces (CF) and the Department of National Defence (DND) are two clearly separate entities. The CF constitute the Armed Forces of Canada and the Chief of the Defence Staff is responsible to the Minister of National Defence for the control and administration of the CF. DND exists to assist the Minister in the management of the CF (i.e., equipment acquisition, etc) and formulating policy relating to national defence. In recent times, there has been an unfortunate tendency to blur the demarcation of responsibilities between the CF and DND, a tendency exacerbated by DND's own insistence on referring to the two collectively as Defence (note the capital D). For the sake of clarity in this report, the operational responsibilities which accrue to the CF will be correctly attributed there, and the support functions of DND will also be so identified.

to be the information highway for sharing data among Government departments and agencies, and the development of High Frequency Surface Wave Radar (HFSWR) systems to provide enhanced coastal surveillance capability. Along with the Canadian Coast Guard (CCG), RCMP, and DFO, the CF has been tasked to increase its on-water presence in accordance with the NSP.

- In addition to being responsible for policies and programs in support of Canada's economic, ecological and scientific interests in oceans and inland waters, DFO is also responsible for improving the safe use of the marine and freshwater environment in order to reduce the number and severity of incidents, such as collisions and groundings, and for providing aid to persons in distress or imminent danger. These latter functions are fulfilled by CCG.
- CCG is being developed as a special operations agency within DFO. It is responsible for satisfying certain marine regulatory requirements for both TC and DFO. The mechanics of these relationships are still being developed. CCG's Regional Marine Information Centres (RMICs) will provide Marine Communications and Vessel Traffic Services and the Long Range Vessel Tracking System envisioned to eventually making full use of Automatic Identification Systems (AIS). AIS is currently in the introduction and evaluation phase of its implementation. CCG is also responsible for aerial surveillance of the coastal waters for fisheries, security, pollution monitoring, and search and rescue (SAR). As an organization, it is a first responder for marine disasters, regardless of origin.
- CBSA is a new organization, which incorporates the key border control functions that were previously spread amongst three organizations: the customs function from the Canada Customs and Revenue Agency (CCRA), the intelligence, interdiction and enforcement functions with respect to immigrants and travellers from Citizenship and Immigration Canada (CIC), and the import inspection at ports of entry function from the Canadian Food Inspection Agency. It is now the body which processes commercial goods, travellers, and their means of transport, with the intent of identifying and interdicting high-risk individuals and goods. In doing so, it works with law-enforcement agencies to maintain border integrity and, engages in enforcement activities with respect to investigating, detaining and denying entry to individuals. It is also involved in gathering intelligence by screening visitors and immigrants. CIC provides it with intelligence on those who are breaking the laws and regulations for which it is responsible. CBSA is currently part of the hands-on, first line of defence with respect to port security alongside the RCMP and local police forces.
- RCMP is tasked to support other Government departments in maintaining border integrity, and with other national and international police and security organizations to support continental security. It is responsible for covering the gaps between the official border crossing points operated by CBSA. Under the NSP, the RCMP have been mandated to increase on water presence; this reverses a steady contraction of the RCMP Marine Division over the last thirty years. The RCMP has both enforcement and intelligence gathering functions

relating to port security and are the lead organization in developing people recognition systems.

The Maritime Security Environment

Evolution of Departmental Cooperation

22. Although many Government departments and agencies have specific jurisdictional responsibilities in terms of the enforcement of laws and regulations that are delimited in statutes and departmental mandates, there is often a geographical and physical overlap in the domains in which the departments exercise their responsibilities. This is nowhere more evident than in the marine environment. Activities on the water, whether in the Great Lakes, the international river boundaries (such as the St Lawrence River), internal coastal waters, the Territorial Sea or the High Seas contiguous to Canada's sea frontiers, are particularly complex as, in addition to diverse responsibilities such as immigration control, fisheries protection and military activity, there is a common demand among the departments for effective surveillance measures, communications requirements and platforms from which to execute their functions and duties. There is immense scope for duplication of resources and concomitant inefficiencies. For many years, this has, in fact, been the case.

23. In addition to whatever other infrastructure was required to support a particular department's mandate, many departments maintained their own fleet of vessels, designed and maintained to meet normal operating conditions. Notwithstanding common government ownership, these fleets tended to operate completely autonomously and independently from one another. In 1962, at the time of the creation of CCG, the Glassco Report noted that there were some 14 Government departments and agencies with some responsibility for the management of maritime affairs and activities operating a total of 13 separate government-owned fleets.⁹ There were several initiatives that arose from the late 1950s onward that were intended to make more efficient use of the Government's maritime assets. Sadly, however, the vast majority of these initiatives were focussed solely on saving demands on the treasury, without a great deal of concern for improving operational capability across the spectrum of governmental responsibility.

24. As an example, an Order-in-Council was put into effect that designated naval officers as peace officers for the purposes of fisheries protection. The reasoning behind this idea was that, if the Navy was to be going about its business in the vicinity of fishery activity, it could be used to supplement the DFO vessels, which were largely limited by speed, endurance and sea-keeping ability from being able to patrol the off-shore fishery effectively. What few appreciated was that, to be effective, a fisheries officer required a great deal of specialised knowledge that was generally not in the purview of naval

⁹ Royal Commission on Government Organization, *Volume 2-Supporting Services for Government* (Ottawa: Queen's Printer, 1962)

training. To illustrate: to most naval officers, one block of frozen fish in the hold of an offshore factory ship looked much like every other block of frozen fish. In time, a more practical solution evolved, in which the Navy assigned vessels specifically to patrols aimed at monitoring active fishing areas, and fully-qualified, and duly-certified Fisheries Protection Officers were embarked to conduct the specifics of fisheries-related boardings and inspections.

25. A better example of interdepartmental cooperation is to be found in the evolution of the Rescue Coordination Centres across the country. The Rescue Coordination Centres (RCCs) were originally established in 1947 under the requirements of Canada's International Civil Aviation Organisation commitment. Canada was divided into four areas: Atlantic, Eastern, Western and Pacific; responsibility for operating the RCCs was assigned to the Royal Canadian Air Force. The program was set up for the coordination of downed aircraft and, if need be, to aid in the Search and Rescue (SAR) of vessels at sea or person lost or in distress. In 1951 it was decided that marine SAR would be broadened and play a more active role, thus the scope of the Atlantic, Eastern and Pacific RCCs was changed to reflect this policy. This was more a reflection of what was already taking place, as opposed to new duties for the RCC. By this time, Marine cases accounted for more incidents than air cases. In 1960, Marine Advisors from the Marine Operation branch of the Department of Transport were added to the staffs of the RCCs and, when the CCG was established in 1962, the RCCs were staffed on a twenty-four hour basis by officers of the CCG, which assumed responsibility for Marine Rescue. In both the Atlantic and Pacific regions of Canada, the RCCs are an active adjunct to the Maritime Operations Centres (MOC) operated by the Navy for the purposes of collecting, analysing and disseminating information on activity within Canada's areas of interest and responsibility.

26. As pragmatic solutions for interdepartmental cooperation were often easier to achieve than restructuring the entire legislative framework upon which each department's jurisdiction was defined, memoranda of understanding were worked out to facilitate interaction. For example, although outside of specific responsibilities for fisheries protection and immigration control, the RCMP were, and are, responsible for the enforcement of Canadian law at sea, subject to such territorial limitations as imposed under international law. However, the RCMP Marine Divisions were not equipped with vessels adequate for operation outside the near-shore coastal areas. Hence, to develop an effective capability to deal with drug smuggling on the high seas and in Canadian territorial seas, a memorandum of understanding was established between the RCMP and the Navy, under which the Navy would provide surveillance and tracking information and, when necessary, embark RCMP enforcement teams in naval ships in order to effect interdiction and arrest of suspicious vessels. The broad authority for this type of activity is laid out under the provisions of Part IV, Article 273.6 of the *National Defence Act* pertaining to Public Service, but the specific processes and procedures were established under the MOU. As the levels of cooperation grew between the RCMP and the Navy, and as the RCMP resources in the Marine Divisions were reduced by successive budget restrictions, a more or less continuous RCMP presence was put in place at the Navy's MOCs; the degree of involvement at each MOC was mostly at the initiative of the local

RCMP Division Commander and the Navy's Commander of Maritime Forces on each coast.

27. The level of cooperation between various Government departments with maritime responsibilities was boosted periodically by the publication of various reports and establishment of commissions, such as the Glassco report mentioned previously. By 1990, the number of government-owned fleets had been reduced to four: the CCG (TC), DFO, the RCMP Marine Division and, of course, the Navy¹⁰. In the structure of the current fleets, the Osbaldeston Report submitted in that year was instrumental in setting the goals for optimization of fleet utilisation.¹¹ In order to achieve this optimization, the Interdepartmental Program Coordination and Review Committee (IPCRC) was formed with the mandate to foster more efficient cooperation and coordination among the fleets. This committee operated for just over a decade, until it was disbanded, 17 September 2001, six days after 11 September 2001. During its tenure, IPCRC did achieve some useful goals in the area of sharing fleet capacity to meet various sovereignty requirements, such as support to the RCMP in the off-shore and increased surveillance of the fishery. Moreover, the subcommittees of IPCRC were able to advance cooperation in the areas of communications and the ability to share common information among several departments. The subcommittee on operations developed, published and promulgated an operations procedures manual that coordinated operations involving both the Navy and CCG. The contribution of other Government departments to the staffing of the Navy's MOCs on an ad hoc basis during the IPCRC era provided the foundation concept for the more formalised cooperative structure envisaged for the new MSOCs, which are discussed in more detail later on in this report.

28. Following the 11 September 2001 attacks, initial steps were taken to improve maritime security by increasing vigilance in the ports and on the seaways. One key tool in monitoring vessel movement was to extend the vessel reporting requirement from 24 hours to 96 hours prior to entering territorial waters, with a requirement for additional information in the report on crew and cargo manifests and the vessel's movement history. This dramatically increased the warning time needed for research about each vessel. Physical security in major ports was upgraded, and inspections of containers increased.

29. As a pre-cursor to PSEPC, an ad hoc Cabinet Committee on Public Security and Anti-Terrorism (PSAT) was formed¹². This committee was made up of ministerial-level representatives from the Privy Council Office, DND, the Solicitor General, CCRA, CIC, TC, DFO, CCG and the RCMP. Of particular interest to the maritime community, the PSAT Committee also proposed to Cabinet several distinct marine security measures. TC was tasked as lead department to undertake a comprehensive threat assessment and a vulnerability gap analysis. CCG and DFO were tasked with increased surveillance of our

¹⁰ CCG was subsequently transferred to DFO, which is now responsible for operating the entire civilian Government fleet.

¹¹ Treasury Board, *All the Ships That Sail—A Study of Canada's Fleets* (Ottawa: Supply and Services Canada, 1990).

¹² With changes to the machinery of government, announced in Dec 03, PSAT has been replaced with the Cabinet Committee on Security, Public Health, and Emergencies.

ocean approaches, and the CCRA was given responsibility to increase security at ports, most particularly in the handling of containers. Funding, as noted above, was committed to these taskings.

30. The Minister of Transport was given responsibility for forming IMSWG. This interagency committee is responsible for presenting mature findings to the Minister of Transport for presentation to Cabinet. It is not clear yet, what role if any PSEPC will play in the oversight of IMSWG.

31. IMSWG was initially given \$60 million over five years to fund essential maritime security initiatives. Thirty-nine million dollars was allotted for the IMSWG contingency fund, \$2 million of which has already been split between DFO, which is developing an AIS for merchant vessels, and DND, which is investigating an upgrade to maritime information data fusion and management (i.e., MIMDEX). A further \$6 million was provided to TC for ongoing threat and port vulnerability assessments, and \$15 million went to the CCG to improve surveillance and navigation systems.¹³

32. In addition to the work undertaken by IMSWG, Government departments and agencies with responsibilities related to law and regulation enforcement at all points of entry to Canada, including seaports, have, in cooperation with corresponding agencies in the USA, formed Canada/US Integrated Border Enforcement Teams.¹⁴ The Integrated Border Enforcement Team (IBET) is a multi-agency law enforcement team that emphasizes a harmonised approach to Canadian and American efforts to target cross-border criminal activity. The importance of IBETs has been heightened by the new reality of terrorism and the need to enhance border integrity. The model is built on the premise of partnership, and on sharing information more effectively to stay one step ahead of criminals and terrorists. Originally developed in 1996 as an innovative method to address cross-border crimes along international land and marine borders between British Columbia and Washington State, IBETs have evolved into a major enforcement success.

33. The original core agencies from Canada and the U.S., which have a direct interest in IBETs, are:

- RCMP
- U.S. Customs and Border Protection (CBP)
- CIC
- U.S. Immigration and Customs Enforcement (ICE)
- CBSA
- U.S. Coast Guard (USCG)

IBETs enable U.S. and Canadian police services and law enforcement communities to work together daily with local, state and provincial enforcement agencies. Both countries

¹³ Avis, Captain(N) Peter, *Surveillance and Canadian Maritime Domestic Security* (http://www.navy.forces.gc.ca/mspa_news/news_issues_e.asp?category=4&title=14)

¹⁴ http://www.rcmp.ca/security/ibets_e.htm

share a common border and common objectives: to ensure that the border is open for business, but closed to crime.

An Assessment of Port Security

Port Security Requirements

34. The specifics of port security requirements are defined in the International Ship and Port Facility Security (ISPS) Code adopted by the International Maritime Organisation (IMO) on 12 December 2003. These requirements were ratified by Canada and promulgated in the Maritime Security Regulations made by Order-in-Council under the *Maritime Transportation Security Act* in May 2004 and brought into force 1 July 2004. The scope of this report is limited to the security of ports; hence, only those sections and provision of the regulations that pertain to marine facilities, that is Part 3 of the regulations will be discussed.

35. For the purposes of the regulations, a port means: (a) a port as defined under the *Canada Marine Act*; (b) a harbour for which a harbour commission is established under the *Harbour Commissions Act*; (c) a public port designated under the *Canada Marine Act* in which a marine facility that interfaces with vessels to which the regulations apply; or (d) a group of marine facilities, in close proximity to each other, the operators of which agree with each other to subject themselves to the provisions of the regulations for the purposes of security.

36. Indeed, under the regulations, the security of ports is established as the collective security of the marine facilities located in that port. A marine facility is a facility that interfaces with vessels subject to Part 2 of the regulations (i.e., vessels in Canada, and Canadian ships outside Canada, that are SOLAS¹⁵ ships or non-SOLAS¹⁶ ships). The regulations do not pertain to facilities that interface exclusively with pleasure craft, fishing vessels, Government vessels or vessels without a crew that are in dry dock, dismantled or laid up. It should also be noted that special provisions apply to “occasional-use facilities.” These are facilities that, in a calendar year, have 10 or fewer

¹⁵ “SOLAS ship” means a vessel that

(a) is 500 tons gross tonnage or more or is carrying more than 12 passengers; and
(b) is engaged on a voyage from a port in one country to a port in another country other than a voyage solely on the Great Lakes and the St Lawrence River as far seaward as a straight line drawn from Cap des Rosiers to West Point, Anticosti Island to the north shore of the St Lawrence River along the meridian of longitude sixty-three degrees west.

¹⁶ “non-SOLAS ship” means a vessel that is not a SOLAS ship, is engaged on a voyage from a port in one country to a port in another country and

(a) is more than 100 tons gross tonnage, other than a towing vessel;
(b) carries more than 12 passengers; or
(c) is towing a vessel engaged in towing a barge astern or alongside or pushing ahead, if the barge is carrying certain dangerous cargoes.

interfaces with vessels to which Part 2 of the regulations apply, where no more than five of these interfaces involve a vessel on a fixed schedule with the facility.

Responsibility Interfaces

37. Although the regulations assign specific responsibilities to security officers within ports and marine facilities and to the operators of ships, the overall responsibility for ensuring compliance and holding local authorities to account resides with the Regional Director General (RDG) of TC.

38. The *Canada Marine Act*¹⁷ of 1998 devolved responsibility for port management and security to local authorities, and the resulting organization for each port was a matter of negotiation between the major stake-holders. Consequently, the actual processes in place differ slightly from one major port to another. In this report, we will examine the regimens in Vancouver and Halifax. Notwithstanding the differences, the Federal Government has committed \$115M over fiscal years 04/05 to 07/08 on a 75/25% cost-share basis to assist all Canada's ports and terminal operators with the cost of strengthening their security systems and programs. This application-based program is applicable to expenses incurred after April 2004 for the purposes of meeting compliance with ISPS Code and the Canadian regulations.

39. **Vancouver.** Security at the Port of Vancouver is a partnership between federal officials, local law enforcement agencies and the Vancouver Port Authority (VPA), working in conjunction with its terminal operators, tenants and community stake-holders¹⁸. Each of some 28 marine facilities has developed security plans. The VPA has put them into a master security plan in accordance with their coordination role. A key element was to ensure the individual plans were sustainable over time. The marine facility operators decided to adopt a common Port Access Card. Many other waterfront land-holders voluntarily did security plans, but they do not have to implement them and they are not coordinated with the rest of the Port.

40. Criminal security and law enforcement on land and water is the jurisdiction of local police agencies with national support from the RCMP. The Combined Forces Special Enforcement Unit (CFSEU) is responsible for coordinating police response to criminal activity on Vancouver's waterfront.

41. TC is responsible for ensuring International Ship and Port Security (ISPS) code compliance in Canada in accordance with the Canadian Maritime Security Regulations and monitoring the entry of foreign vessels to Canadian waters.

42. Border protection is the responsibility of the Canada Border Services Agency (CBSA), Citizenship and Immigration, supported in marine frontiers by the CCG and DND.

¹⁷ <http://laws.justice.gc.ca/en/c-6.7/18383.html>.

¹⁸ Port Vancouver, *Port Security Brochure*, 2004.

43. The VPA, its terminal operators, port tenants and the port stakeholder community are responsible for the security of port property, personnel and infrastructure.

44. **Halifax.** Halifax consists of 14 marine facilities, and, it appears the evolution of the port security regime is proceeding in a similar fashion to that of Vancouver. However, as of mid-October 2004, some aspects, such as the Port's Master Security Plan had not yet been fully developed, and the question of common Port Access Cards has not yet been fully addressed.

Security Assessments – Considerations for the Port Security Regime

45. The regulations make provision for security assessments at marine facilities and the collective security of the marine facilities which comprise a port. Indeed, these provisions for compiling security assessment information, the elements that comprise security assessments and the matters to be taken into account, and the requirements for conducting on-site surveys and vulnerability assessments appear, at least from a check-list point-of-view, to be relatively complete. However, the greatest weakness lays in addressing all the vulnerabilities identified and providing for a clearly defined hierarchy of decision-making and direction in response to a perceived threat to security. In other words, although the regulatory framework is comprehensive, it is evident that the operational capability necessary to identify and respond to emerging threats is still under development.

46. **Defence in Depth.** Like all potential threats the best way to deal with them is at their point of origin, or at least from the greatest distance possible from the intended centre of damage. Thus, the specific question of port security must fit into the broader geographical context of maritime security, including coastal, ocean approaches and offshore defence. In this regard, the regulations have worked from the inside out, whereas the most effective means to deal with the question of port security is from the outside in. From this point-of-view, the regulations are necessary, but not a sufficient condition for real security in the marine environment.

47. **Comparison of Seaports and Airports.** A seaport is fundamentally different from an airport. The primary difference is, excluding small civil aircraft, the vehicles used in the air industry are concentrated in the hands of a relatively small number of responsible operators, and their locations are well-known, whether on the ground or in the air. The aircraft take-off and land at well-bounded facilities, and they are more or less immune from interference while in transit between terminals. Hence, if the air terminals are secured in terms of physical security, and the people and cargo entering the secure area are thoroughly sanitised from a security point of view, the whole operation can be rendered safe. This is not to trivialise the difficulty of producing the high level of reliable security necessary to meet this condition; however, it will serve to illustrate the fundamentally different problem associated with seaports.

48. A seaport is a much larger and more complex set of infrastructure than an airport, and, as indicated in the regulations, a port, particularly a large one, is really a loose collection of a number of marine facilities. Moreover, many ports are in the centre of cities and are used not just commercially, but for recreational activity, and public access to the waters of the port is taken as a fundamental right by the residents of the city. A key result of this is, while marine facilities are usually secured by fences and other physical measures on the landward side, on the seaward side they are usually directly accessible.

49. Furthermore, the sheer volume and diversity of freight shipped by sea compounds the difficulty in ensuring the security of cargo. For example, annually, the Port of Vancouver handles between 60 million and 70 million metric tonnes of cargo and trades with more than 90 economies.¹⁹ In 2003, the Port of Vancouver handled more than 1.5 million containers (TEU).²⁰ This quantity is expected to grow to three times this number over the next five years. However, the methodology of handling cargo does provide some potential “choke-points” to facilitate screening and inspection. As discussed in more detail below, smart, automated detection equipment can be applied to this task to minimise human involvement and corresponding labour costs.

50. The fundamental distinction, from a security point-of-view, between aircraft and watercraft is the degree of scrutiny to which they are subject in their day to day operation. Although modern technology, such as global positioning systems and automatic tracking systems, make it possible to continuously account for the location and activity of a vessel, these systems are not yet the norm in large merchant ships, let alone in the innumerable fishing vessels, small working craft and pleasure boats that ply the world’s oceans. In essence, unless a vessel is being monitored visually or by radar, it is essentially invisible from the time it leaves one secure marine facility until it arrives at the next. To return to the aircraft analogy, if an aircraft leaves one terminal in a safe condition, unless there has been a failure in the ground-based security prior to its departure, as there clearly was in the 11 September 2001 events, it will arrive at its destination in the same condition. This, however, is not the case for ships and boats. On the high seas or in the many secluded inlets and coves around Canada’s shoreline, there are infinite opportunities for vessels to engage in illicit activity or embark dangerous materials with which to threaten the security of their port of destination.

51. The discussion to this point has been focussed on vessels engaged in international voyages (i.e., vessels to which the ISPS Code applies). The vast majority of vessels operating in Canada’s waters do not fall into this category. Vessels that are not covered by the provision of ISPS are not subject to any directed formalised scrutiny. They include all types and sizes of pleasure craft, commercial vessels operating exclusively between Canadian ports, fishing vessels, and the many freight, car and passenger ferries that operate in Canada. In 2003, the BC Ferries Corporation operated 37 vessels calling at 47 terminals; the fleet carried 21.4 million passengers and 8.3 million vehicles.²¹ As of

¹⁹ <http://www.portvancouver.com/statistics/>

²⁰ TEU: Twenty foot Equivalent Units

²¹ BC Ferries Annual Report 1003/04 (http://www.bcferrries.com/files/PDFs/BCF_AR2003.pdf)

mid-November 2004, there were no apparent measures being taken to screen passengers or vehicles embarked on the ferries.

Requirements for Port Security

52. **Threat Analysis.** A discussion as to what constitutes the nature of threats to ports is relevant to this report. Insofar as practicable, the analysis of the threat will be focused on the high-level and general, as opposed to the detailed and specific. However, a series of specific and detailed scenarios will be required to exercise the plans and organizational structure being developed to address port security issues.

53. **From Sea.** The threat posed by a ship can originate from three sources: the threat from the ship itself (e.g. something attached to the ship as a whole used as a weapon), the cargo, or the crew. Once in the harbour and alongside it is possible for something attached to the ship or in the cargo or a member of the crew to constitute a threat. Some ports have a roadstead or holding area where ships are required to wait until alongside facilities are available. This offers the security system an opportunity that is not as readily available to ports where vessels can proceed directly alongside on arrival.

54. **From Ashore.** The threat posed from ashore can originate from four sources; however, all can be controlled, as they have to pass through a physical barrier on the land-side of a controlled port facility.

- **General Public.** The general public may form the main threat to ports from ashore. Individuals can carry and deliver a variety of agents or items that can cause damage to the port infrastructure or its workforce or both when they gain access.
- **Passengers.** As in the airline scenario, passengers, particularly those willing to forego any consideration of their own safety, can pose a significant threat to the port and marine facilities, as well as to the ship in which they embark.
- **Workers and Equipment.** The workforce and equipment that pass in and out of secure areas pose a significant threat. Workers can carry hazardous materials, which can also be secured or hidden on equipment that passes in or out of the port. It is an unfortunate fact that the proportion of waterfront workers with a record of criminal activity is higher than the general population, and, for reasons which are difficult to comprehend, unions have historically objected to comprehensive security measures at marine facilities.
- **Cargo.** Likely, the most significant threat posed from ashore will be by the cargo that is transported through a port. This is valid either in the landing from a ship or the delivery to a ship or while the cargo is in the port storage area.

55. **From the Air.** The threat posed from the air could originate from a variety of places (e.g. from land, from an airborne vehicle, or from a ship). The nature of the threat could also use a variety of platforms, from an airplane manned or unmanned, to a

balloon, to a kite or to a model airplane. The platform itself could be the weapon, or, in the case of larger platforms, it is more likely that the weapon would be dropped from the platform.

Intelligence

56. A fundamental requirement of any activity that crosses international boundaries and one where commerce is the prime motivation is a functioning and reliable intelligence network. Canada is a member of a variety of international organizations that share intelligence and a special relationship on the sharing of intelligence between Canada and the USA is in place. Thus the key objective of the NSP is to harmonise this external intelligence information network with the local, regional and national intelligence gathering organizations within Canada.

57. Counter-terrorism efforts require an integrated approach to help ensure early detection and prevention of any potential threats to national security. The RCMP has refocused its National Security Intelligence Sections (NSIS) to become Integrated National Security Enforcement Teams (INSETs).²² The purpose is to increase the capacity for the collection, sharing and analysis of intelligence among partners with respect to targets that are a threat to national security; to create an enhanced investigative capacity to bring such targets to justice; and to enhance the partner agencies' collective ability to combat national security threats and meet all specific mandate responsibilities.

58. INSETs are made up of representatives of the RCMP, federal partners and agencies such as CBSA, CIC, CSIS as well as provincial and municipal police services. INSETs were originally formed in Vancouver, Toronto, Ottawa and Montreal. Through shared federal, provincial and municipal resources, the INSET members are better able to track and put a stop to the criminal activities (major or minor offences) of terrorist groups or individuals, who pose a threat to Canada's national security. This type of increased capacity enables INSET members to work with their partners nationally and internationally towards the common goal of detection and disruption of potential terrorist threats.

Surveillance and Monitoring (Collecting Information)

59. As an adjunct to intelligence collection, it is necessary to commence the surveillance network as far from the port of destination as possible. To be successful, surveillance is the integration of many sensors into a common geographical referenced framework. Surveillance can be general in nature or in direct response to a known or suspected threat.

²² http://www.rcmp.ca/security/insets_e.htm

- **At Sea.** A variety of means and sensors are available for integration into a surveillance framework. These vary from terrestrial, through surface search, to underwater sensors. They can be enhanced by direct surveillance from an airplane or a surface or subsurface vessel. Uninhabited Air Vehicles (UAVs) and Autonomous Underwater Vehicles (AUVs) are more modern versions of direct surveillance platforms.
- **Alongside/At Anchor.** In addition to conducting surveillance of vessels while underway, there is necessity to monitor the vessels while alongside or at anchor.
- **Ashore.** Surveillance on land tends to be more in the line of sight domain with cameras, video or the human eye. This surveillance needs to be enhanced at night by either night vision devices and/or lighting and can be augmented by dogs or semi-autonomous surveillance robots. For objects, signal emitting transponders can provide an enhanced tracking ability.

60. As sophisticated as some surveillance measures might be, there is a significant contribution that can be made to marine security by an alert, informed and observant public. As an outgrowth of the Coastal Watch Program initiated by the RCMP in the early 1990s to deter narcotics smuggling, a new Border Integrity Coastal Watch²³ Program has been inaugurated to increase public vigilance in a broader security application. The initial trial of this program was sponsored by the Detroit-Windsor IBET.

Collating Information

61. Information from intelligence sources and sensors of all sorts needs to be sorted and collated into useable groupings and tested for reliability, timeliness and accuracy.

- **Fusion capability.** The process of turning data into information and information into knowledge is referred to as fusion. To fuse information, it must be vertically integrateable, either in a geographic or other common framework. For surveillance, the framework tends to be geographic. However, information that doesn't fit into this framework can be still used to annotate contacts or targets.
- **Maritime Security Operations Centres (MSOCs).** As a result of the Government of Canada promulgation of the NSP, there has been direction to commission new MSOCs on both coasts. These Centres will be headed by the



²³ http://www.rcmp.ca/security/b_integrity_coastal_e.htm

Navy and will include staff from CBSA, TC, the RCMP and CCG. The MSOCs will have the authority and capacity, through interagency staffing, to bring to bear all civilian and military resources necessary to detect, assess and respond to any maritime security threat. They will be networked with the CCG's vessel traffic and communications systems and with the new Government of Canada Operations Centre in Ottawa. The inclusion of all information sources such as the Cooperative Ocean Information Network Pacific (COINPac) will be important for situational awareness. The MSOCs will be a key node in the fusion process, and they are critical to the Port Security Model proposed below.

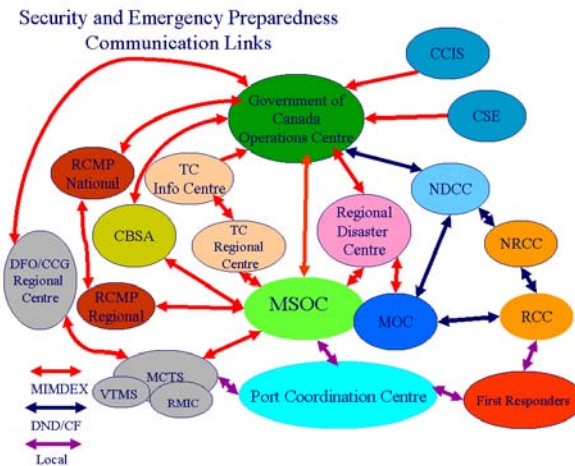
Disseminating Information

62. Information, once turned to knowledge, needs to be transmitted to parallel operations centres to ensure a common level of understanding for the decision makers.

- **MIMDEX** (Maritime Information Management and Data Exchange) is a new

Government of Canada interdepartmental and interagency information exchange network for those that have a role to play in the maritime security field. It will bring information in and out of the MSOCs for each member and vertically to the headquarters of each member and the Government of Canada Operations Centre in Ottawa. MIMDEX will be the information highway that links

the MSOC to the Government of Canada Operations Centre. It will also link it to the Port Control Centres in its region. MIMDEX will also be the primary link between the various departmental representatives assigned to the MSOC and their superiors though their individual operational structures which it in turn will also link with the Government of Canada Operations Centre. It will be an unclassified net with each of the users controlling the information that they enter into it. In due course there will be a Government Secret Net that will enable departments to exchange classified information. The MIMDEX project is the responsibility of DND/CF and has completed the proof of concept phase of its development. A budget of \$8 million has been allocated to have it in place in 2007.²⁴ MIMDEX is another key component of an integrated Port Security Model



²⁴ According to discussions with DND officials, MIMDEX is still in project definition phase and has not yet been approved for implementation. MIMDEX provides linkages to operators / analysts and will likely provide connections to the Government Operations Centre. The Regional Disaster Centres concern inter-governmental coordination and there is no current plan to have MIMDEX in these centres. MIMDEX will operate at the "protected" level.

Response Capability

63. Once a threat, real or potential, is detected there needs to be a response to counter it. Responses in most case need to be pre-planned and exercised, particularly when they are interdepartmental or interagency.

- **Differentiating Terrorism from other Public Safety Phenomena.** There are many public safety phenomena such as environmental hazards and criminal activity that fall into traditional response categories; however, terrorism represents deliberate attempts to destroy property and inflict injury and death for the purposes of political coercion. While some measures to prevent or address the outcome of terrorist attacks will be similar to those for criminal activity or disaster mitigation, the key difference lies in determining whether the outcome is the effect of a covert attack, and whether the attack is one in a series or a stand-alone event.
- **Decision-making and Direction.** This is the horizontal and vertical framework whereby the activities of participants assigned to respond to an incident or threat are synchronized. This framework also supports the decision-making hierarchy such that all participants know who is directing and making decisions; that is, it defines authority and responsibility. This framework needs to be frequently exercised and the primary decision-makers need to participate in the exercise scenarios. A long-recognized principle of crisis management demonstrates that, in order to be effective, plans must be exercised regularly and thoroughly, with as much realistic detail as possible, including the deployment and operation of actual response assets.
- **Coordination and Communications.** Coordination is the means whereby all the various assigned elements operate in harmony and is best achieved when activities have been previously thought out and exercised such that responses are virtually pre-planned. The basis for effective decision-making, direction and coordination lies in a proven communications network, with well-established procedures and protocols for exchanging information between all participants.

An Integrated Port Security Model

64. It is fundamental that Port Security be positioned within some larger security framework. This framework will also have to include the ability to communicate with the regional and national decision-making hierarchy, so as to ensure unity of direction and control.

65. Below, this report will address the elements required to establish an integrated port security regime. However, in anticipation of such a discussion, it is useful to consider the essential elements of such an integrated system that are already in place or being developed.

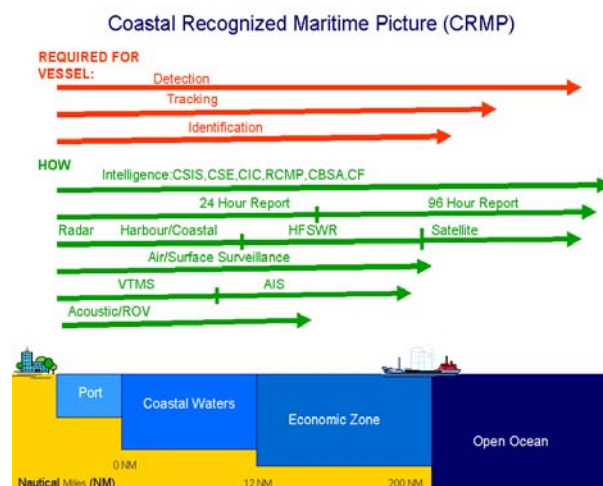
- Government of Canada Operations Centre
- Integrated Threat Assessment Centre
- INSETs
- IBETs
- MOCs
- MSOCs
- RCCs
- Marine Communications and Traffic System (MCTS) Centres: Operated by CCG, these centres are responsible for regional Vessel Traffic Management Systems (VTMS), Regional Marine Information Centres (RMIC – broadcast of weather and safety advisories) and pollution monitoring and response.
- MIMDEX.

66. Throughout the text, figures used demonstrate the concept of the integrated port security model and the communication links between the port, marine and national security decision authorities necessary for such an integrated model to operate effectively.

A Generic Description of a Layered Integrated Port Security Regime

Maritime Security Operations Centres and the Coastal Regime

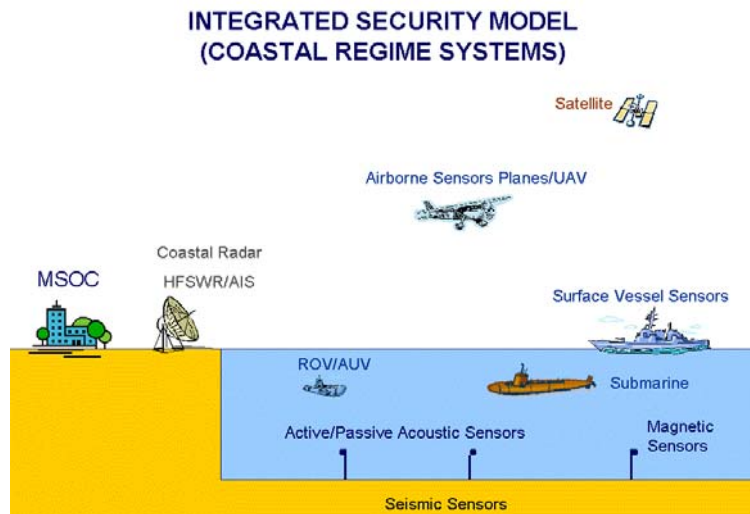
67. Although still under development there can be little doubt that the key element of the integrated model is the MSOC, where all-source sensor and intelligence fusion can take place. By virtue of the presence of the main Government of Canada departments and agencies involved in Maritime Security, the MSOC, collocating and sharing information with the Navy’s MOC, will be able to perform the function of the coastal decision-making and communications centre, both vertically to national authorities and horizontally throughout the coastal region. Thus, this will be the hierarchical centre that will fulfill the current void for the Port authorities.²⁵



²⁵ NOTE: Although consistent with the fundamental intent for the MSOC, the vision for these centres incorporated in this model exceeds the current mandate for the project. According to discussions with DND officials, MSOCs will provide a physical space for operational coordination; however, they will not

68. For the MSOC, it is here that the regional contribution will be made to the National Recognised Maritime Picture (NRMP), which will be collated, fused and maintained through the National Defence Command Centre (NDCC) in Ottawa. Each of the departments (CBSA, TC, RCMP and CCG) and the DND/CF presence will bring their own information and intelligence and fuse it into the Coastal Recognized Maritime Picture (CRMP) that will prepare it for decision-making, both for the region and nationally.

69. The CRMP must start as far out to sea as possible. Ideally, the port of departure forms the first point of available information for any vessel. In addition to open source information, including the internet, surface observation systems, such as satellites and long range patrol aircraft, and their various sensors should form the basis for the first tracking and identification of contacts as they begin to approach the coast. The addition of information from the USA and/or through a future NORAD mission in the integration of the North American maritime surveillance picture should be



able to significantly enhance this long range CRMP. At the 96 hour call-in point for all international arriving vessels, the objective should be to have identified and track all approaching contacts. The CCG VTMS, the new HFSWR, once installed, and the AIS are key tools in this architecture. From that point, all contacts should be retained under positive identification until they reach their port of disembarkation.

70. If any contact is known or suspected of being a threat, it must be dealt with in a different manner and neutralized either by policing or other action. It must be kept under continuous surveillance; it must be isolated from the other vessel traffic and kept at a distance, until it can be neutralized.

71. Underwater sensors of various sorts off the coast or in the approach waterways could be used to enhance the tracking and add to the knowledge about vessels of interest.

72. The CRMP must include the ability to continuously monitor vessels above the surface of the water, so that they would be observed if they were to launch a vehicle or

actually have responsibility to coordinate operations. Nonetheless, the NSP identifies MND as the lead minister for the coordination of on-water response to a marine threat or developing crisis, so it is considered likely in the long-term that the role of the MSOCs will converge with the scope envisioned here.

weapon. This ability needs to be continuous from the identification point and, in particular, when within the sight of land.

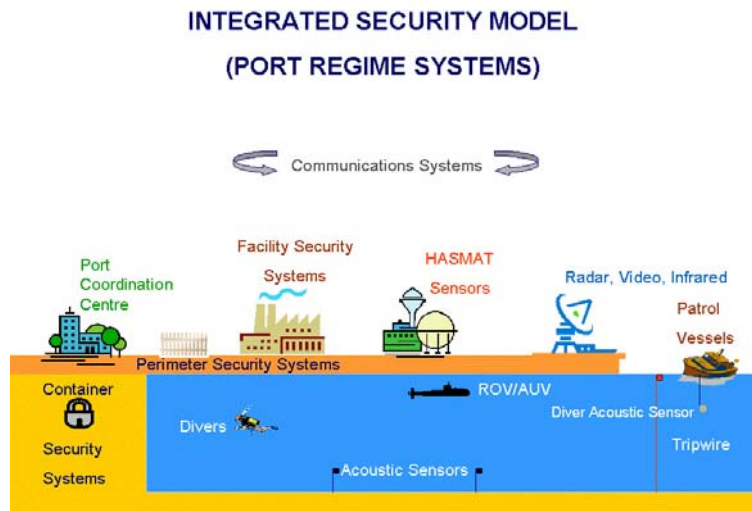
73. Furthermore, as there is always the possibility of a vessel dropping off an object, it is imperative that a complete survey of the seabed be completed for any territorial or inland waters likely to be transited by vessels. This survey will need to be stored in an easily accessible secure database and periodically verified. The ability to verify or respond to potential threat or intelligence will need to be available on relatively short notice. Then, if an object is located, AUVs, remotely operated vehicles (ROVs), manned submersibles or even divers will need to be available to respond as appropriate in order to neutralize it.

74. All territorial and coastal inland waters that are regularly transited by vessels of any kind will need to be included in the CRMP, so that there is a constant awareness of the overall activity along the coast and in the passages around the coast²⁶.

75. **The Port.** The Coastal regime will keep track of vessels right up to the entrance to a port or roadstead, much as the VTMS system does now. The hierarchical organization of ports is now in place and, where necessary, the ISPS Code has been implemented by virtue of the Canadian Marine Transport Safety Act.

76. The first line of defence for a port is the integrated coastal security regime (i.e., starting as far from the port as possible). Given that all threats will not be identified and neutralized at a distance, it is necessary to have the capability to deal with them at the port. A risk analysis and the related cost effectiveness will dictate which capabilities need to be continuously available “24/7” (to use the currently fashionable abbreviation) and which can be “on-call” as prearranged and exercised.

77. **Port Coordination Centre.** It is clear that the port will need a continuous focal point for security, and security-related information gathering and coordination. It should also have a decision-making mechanism for those decisions within the responsibility of the port. This centre will need to be able to receive direct feeds of information from agencies that operate in different jurisdictions like a MCTS Centre and be able to directly monitor the physical



²⁶ While there is a level of awareness of on-water activities in the Great Lakes and other inland waters, the focus of the MOCs / MSOCs is the territorial sea and approaches. Challenges specific to Great Lakes and waterway is currently being examined by the IMSWG.

security of approaches and operations of facilities within the port. This centre needs to be recognized as the initial response reporting point for port-wide anomalous activity and reporting for facility security guards. There will need to be scripted reaction for those that work in the centre, so that correct action is taken to generate immediate response appropriate to the situation. Although previously mentioned, the necessity to regularly and thoroughly exercise decision-making capability and reaction resources cannot be over-emphasized.

78. **Harbour Floor and Acoustic Measures.** Firstly, it makes sense that all ports have a complete and accurate underwater seabed and jetty survey, which is stored in an accessible database. Then, periodic verification surveys or those in response to some intelligence or threat can be completed by either a continuously available or “on-call” capability and compared quickly with the database. Thus, a variety of sensors and capabilities are going to be necessary. The Navy is already conducting work in this area on a limited basis; hence, it is important that the data on the seabed acquired for any other purpose should be sufficiently detailed for mine counter measures (route survey) actions and the database be in a format useful to the Navy (or agency conducting the follow-on route survey activity/comparison).

79. The baseline surveys will need to be repetitive in nature and done by towed high-definition, multi-beam sonar. As they look to the side they can survey right up to the shoreline and in the vicinity of jetties; although, it might be necessary to add video coverage of complex jetties to the resultant data set. Technology is moving quickly in this field and AUVs and ROVs also have the ability to conduct detailed surveys.

80. Periodic verification and response to intelligence or threat can be dealt with by a high definition fixed or mobile sonar system on a vessel that can handle the site specific scenario in response to identifying any anomalies and, if necessary, remove or defuse them. ROVs, AUVs or even divers will likely need to follow to positively identify and, if necessary, defuse the anomaly or object.

81. The storing and management of the seabed data sets can either be by the Port Authorities themselves or under contract, likely in combination with the enterprise that conducted the surveys. Most important will be the security of the data, followed by its availability.

82. As an additional underwater security measure, in certain ports or anchorage areas, it would be useful, to have a ship bottom identification system. This could be a combination of visual and high resolution acoustic sensors that are upward-looking that would aim to identify, in real time, any evidence of unusual attachments on a ship’s bottom. Any such anomaly would be investigated further by an ROV, either with the ship at anchor or alongside.

83. It is also possible to threaten a ship in port by a device attached by an underwater swimmer. To counter this threat, a fixed system of high definition sonar would need to be installed for the parts of a port or anchorage where there is such a risk on a frequent

basis. Alternatively, the availability of a portable or mobile system could provide a degree of defence where there is much lower level of risk. Cruise ships and those carrying dangerous cargo would appear to be those most likely at risk. Along with this defensive capability, there must be the ability to respond quickly to the threat itself, to close it and, if necessary, to communicate, and potentially neutralize or apprehend the swimmer or deal with any explosive device attached or dropped by the swimmer.

84. **Surface and Air.** Surveillance of vessels will need to be positively maintained once they enter a port until they come alongside. Depending on the state of devolution of the port this will remain with the CCG or be done by the Port Authority. The degree of positive radar, visual or other surveillance will depend on the type of port and the measure of risk. Ports like Vancouver will need to maintain a continuous, fully functioning, radar system for positive identification and observance.

85. Other movements, like ferries, within a port will also need to be positively monitored in a coordinated fashion. Radar and AIS will provide a management means of doing so.

86. A response capability to criminal activity or threats brought about, by or on vessels, whether moving in the port or alongside, will need to be available on a continuous basis.

87. Ship-launched air threats are possible, but, the risk would have to be considered low, unless supported by intelligence. However, the risk of an air threat originating from other sources has a potentially higher probability of occurrence. Many ports have monitored air control zones to provide for the safe operation of float planes which would allow for the detection of unauthorized air vehicles. Several also fit within the nearby main city airport controlled airspace. Plans to counter airborne threats are generally part of the overall security umbrella for the nation; however, for port security, no matter how low the risk, these plans need to be integrated with the port security plan.

88. **Marine Facility (The Terminal).** Marine Facilities or Terminals have a special recognition in the ISPS Code, and the security of their land perimeter needs to be assured. Such facilities or terminals are required to control access to restricted areas, usually by having worker recognition (currently a photo pass), control the movement of vehicles and goods and services in and out of the terminal (varying degree of control depending on the MARSEC level) and perimeter securing fencing. Security equipment and services tends to include continuous perimeter monitoring cameras, sometimes with remote zoom and directional control. Facilities have security guards and a monitoring and communications office. In time, these individual facilities will have to be integrated into the larger marine security operational network.

89. It should be noted that even relatively sophisticated perimeter security systems can be overcome, if over-reliance is placed on technology alone. For example, thieves recently defeated a fence and camera system, a minimum requirement under the ISPS

Code, by stealing the cameras before breaching the fence and making off with material from a container handling facility on the West Coast.

90. A response to criminal or other activity within the facility or around its perimeter, land and water, needs to be recognized and responded to in a timely manner.

Scaling the Model for Regional, Local and Occasional-Use Ports and Marine Facilities

91. **Regional Port.** Simple reality dictates that resources must be allocated judiciously; it is a matter of determining what measures are adequate to meet the most likely and the most dangerous events. Clearly, the large, regional ports cannot afford a failure in security, not only because of the direct damage that may be sustained, but also because of the economic impact on the nation, as these ports represent Canada's portals for the life-blood of international trade. Moreover, as ports like Vancouver, Montreal and Halifax serve as conduits for the large American import and export market, the impact of a security failure would be devastating for the future operation of the ports in this capacity. In fact, even perceived weakness in the security measures of the ports could result in the redirection of goods away from these facilities to alternatives in mainland USA. Consequently, the regional ports must be capable of deterring, detecting and responding to the gamut of security threats promptly and reliably on a continuous basis.

92. **Local and Occasional-Use Ports.** For the local ports and less frequently visited occasional-use facilities, the key is in having a good level of infrastructure security and the ability to monitor the approaches. For enhanced security, particularly for the underwater capability, they may pool or share the defensive and response capabilities. These capability packages could be owned and shared or be "on-call" and contracted out on some sort of standing offer contract like the oil-spill response is contracted to Burrard Clean Operations. As a threat is detected or perceived, there needs to be detailed plans for deployment of the necessary resources to the location in a timely manner. In order for this to be effective, the triggers for the decision-making process must be tied to the most advanced warning that can be provided through the defence-in-depth concept. In essence, the appropriate response capability that needs to be maintained to meet the specific requirements is a speed-time-distance problem that must be analyzed to ensure that a reaction commensurate with the probability and consequence of an event is maintained at all times.

93. **Cruise Ship Terminals.** For ports, other than regional ports, that have regular visits by cruise ships, given the likely dire consequence of error, it would be logical to provide a complete defensive and response capability for that terminal. For the occasional cruise ship visit, an integrated security package, including additional staff (likely maintained by "on-call" or standing offer contract), needs to be deployed for the duration of the visit.

Analysis of East and West Coast Industrial Ability to Meet the Model

94. Attached at Annex A to this study is a database of East and West Coast Canadian companies with the potential capability to participate in the industrial requirements of the port security sector. This list is not presumed to be exhaustive, but should be taken as representative of the skills, products and services that are available in Canada to address security requirements. The companies cover a broad range of capability as can be seen in the table, from the provision of simple security measures, such as chain-link fencing, to cutting-edge, high-technology sensors, such as underwater swimmer detection devices.

95. It should be noted that several large multinational companies purport to have models for integrated port security systems that largely correspond to the scope of the coverage envisaged in this report. Many of these multinational companies have Canadian representation in the form of wholly-owned subsidiaries or affiliated companies. It is noted, however, that much research and development activity is ongoing in the USA by federal government laboratories and in industry, and to some degree in Canada, into products that could meet various elements of the integrated port security system. It is also evident that each port is different and any system would require a degree of tailoring to best suit that port. Furthermore, there are several SMEs with dissimilar products or services that have differences in levels of capability and cost but that might, by virtue of the geography of the port or coastal area, provide an equally good or sometimes better outcome. Thus, there is no single solution or product that can be said to be best all of the time. Indeed, it is likely that the key problem will be the level of integration of the various sensors and services that will determine the degree of efficacy. This capability is unlikely to be available off-the-shelf and will require additional funding. The sophistication of the integration will determine the level of funding required.

96. One method that may be applied to the development of the required integrated security model is that of the technology demonstrator. In this case, the major stakeholders of the security responsibilities for a regional port would participate in a planning exercise in which a model for the observe-orient-decide-act cycle for an integrated marine and port security regime would be developed (or confirm the validity of one that is proposed). The second stage would involve construction of a series of technology demonstration projects, managed and funded as appropriate, in which the requirement for local and national SME participation could be balanced against existing integrated security models. Each technology demonstrator would address specific potential threat areas but include the capability to add additional sensors ultimately working toward a fully integrated model. For example, a demonstrator could focus on securing a cruise ship terminal from a variety of attack vectors or the underwater problem, or low cost integration of radar and AIS coverage in confined waters.

97. If it is intended to involve a highly developed SME, then it might become difficult to involve a series of less developed SMEs; however, this can be addressed through the definition of requirements for their participation in the request for proposal and the approval process could be weighed toward the participation of a large number of SMEs.

This has, indeed, been common practice in establishing industrial regional benefits as a condition for participation on Crown projects.

Conclusions

98. As mentioned, there are good economic incentives for improving the perception and reputation of Canadian ports. Having good security will ensure the viability of the ports as economic engines for Canada. It will, furthermore, meet the test of due diligence, if anything negative were to happen in the United States due to the passage of cargo through a Canadian port. Additionally, the work of Canadian companies in providing the products and services that underlie this reputation will open markets in the marine security sector in the global arena. This report contains some suggested fields of endeavour to which Canadian companies may wish to apply themselves. At the risk of elucidating the obvious, companies that successfully develop technology, products and services for the Canadian marine and port security market are likely to have significant success in addressing similar requirements internationally.

Decision Making

99. It is evident that, although the regulatory environment for marine security has been reasonably well-defined, there is a significant lag in developing the corresponding operational capability to meet the requirements of the regulations. Several excellent programs have been developed by departments and agencies with responsibilities under legislation and the regulations, and there have been some initial steps toward enhanced cooperation between agencies. However, the logical step of developing a fully integrated approach to the six maritime issues identified in the NSP has yet to be taken.

100. The first step toward integrating operations should involve the definition of relationships among the various operations and information centres used by many departments and agencies, and establishing an agreed decision-making hierarchy. Clearly, at the regional level, the MSOCs will be the key focus, and additional policy work is required in developing the capability to meet the requirements of all stakeholders for decision-making and crisis management. The CRMP is considered to be a crucial concept as the basis for the MSOC and an area which demands a high priority in determining the Statement of Requirement for the Centre.

101. Port Coordination Centres are an important new concept for executing local decision making, coordinating the security efforts of the marine facilities that comprise a port and integrating the local levels into the regional and national decision making matrices.

Coastal Regime

102. The port security regime must start as far away from the port as possible and it must be integrated into an entire coastal regime that ensures continuity of coverage of all waters and contacts and continuity of decision making.

- Surveillance monitoring in the form of AIS, HFSSWR, and coastal radar needs to be integrated into the CRMP to monitor vessel movements at all times, from entry into Canadian waters to final arrival at a marine facility. Where surveillance sensors are not currently available, a minimum of AIS and some form of radar should be installed. Remote sensors, such as commercially available satellite information, will be valuable inputs to the CRMP.
- Insufficient attention has been accorded to underwater surveillance. Much thought and effort needs to be given to meeting the potential underwater threats. This includes a complete bottom survey of all regularly travelled routes, the maintenance of the subsequent database and its occasional verification.
- Concern over the apparent lack of security of ferry systems in general, including the BC Ferry System, needs to be addressed.

Port Regime

- There can be little doubt that regional ports need a complete seabed and jetty survey, including the management of this database, as well as a combination of fixed and deployable systems and rapid response capability.
- Other ports may pool or share the defensive and response capability based on an assessment of risk versus time and distance. These capabilities can be owned and “on-call” or available through a standing offer contract. Particular attention needs to be paid to cruise ship visits in occasional ports where an integrated security package, including additional staff, needs to be deployable for the duration of a visit.
- Cruise ship terminals which are regularly visited need to be protected with a complete integrated security package.
- Personnel screening for port workers must be significantly enhanced, with a view to achieving the same standards as those required for airport workers. Face recognition and other biometric technologies are important to complement screening checks by ensuring the identity of workers corresponds to background information.
- Security equipment of all kinds must be continuously upgraded to counter concerted efforts to defeat existing systems.
- Improved sensors must be intelligently employed in cargo handling in order to increase the probability of detecting explosive, biological, chemical and radiation threats.
- Technology exists for rapid, non-intrusive scanning of materiel using vapour detection (sniffers), imaging and pattern recognition equipment that can be

employed effectively at “choke-points” such as boarding ramps, cargo handling cranes and conveyor systems and bridges.

103. Technology Demonstrators are a useful vehicle for defining and refining new operational, technical and scientific requirements. Used in conjunction with realistic, real-time exercises, including actual deployment of all response resources, these represent the only thorough way to assess the efficacy of pre-planned responses and the completeness of preparations. In this case, they might be grouped together in a variety of opportunity circumstances, but, whatever the format, they should allow for the addition of other sensors and integration, so that the classic “plug and play” circumstance is in effect.

Summary of Industrial Opportunities

Coastal Regime

- Inclusion of terrestrial sensor information into the early development of the long range CRMP.
- Integration of new sensor derived information like the HFSWR network into the CRMP.
- Development and inclusion of decision aids into the MSOCs.
- Integration of radar and AIS received information into the voice reporting transmission system in the coastal areas currently devoid of such information.
- Where significant surveillance gaps exist in coastal waters and there is no voice reporting transmission system installed, as a minimum AIS and some form of radar be installed along with the ability to include derived information into the CRMP.
- Underwater sensors and bottom topography surveys to complement naval route survey work.
- AUVs/ROVs and potentially manned submersibles to respond to potential threats.

Port Regime

- It is likely that as the Port Coordination Centre develops further there will be a need for architecture improvement to enhance communications, the integration of more information and decision-making processes.
- Ports will need a comprehensive seabed and jetty survey, which is stored in an accessible database. It is likely that more than one sensor will be required and, given the unique features of each port, different ones will likely be used. The resultant data can be managed by the port or under contract.
- High threat facilities like cruise ship terminals will need to have permanently fitted underwater detection sensors. Regional ports, likely depending on geography, may choose to fit sensors to cover the underwater threats solely in the high threat areas or the port as a whole.

- There may be occasions where high frequency sonar fixed on a vessel may be best to respond to seabed anomalies or intelligence. They may be used in conjunction with AUVs/ROVs, or even divers, to respond, if something is found.
- There will be occasions where a very light portable sonar, recorder and communication hydrophone deployable on fast RHIB type boats will be needed to respond to an underwater intruder situation.
- A ship bottom identification system of upward looking visual and high resolution acoustic sensors capable of being monitored in real time would be of significant value at the entrance to roadsteads or harbours.
- Depending upon particular ship security assessments, there is a probable requirement for portable, over-the-side, underwater intruder detection systems.
- AUVs/ROVs will be useful to investigate a variety of situations, including ships bottoms.
- There will be opportunity for the installation of integrated radar and AIS monitoring systems in some ports.
- Enhanced screening systems for port worker access control, including face recognition and biometric technologies, will be required with the next amendment to the Marine Transportation Security Act.
- Facility security systems, as prescribed to meet the requirements of the ISPS code and the Marine Transportation Security Act, will need to be periodically upgraded, further integrated into the facility monitoring centre and, in due course, electronically connected to the Port Coordination Centre.
- Remotely operated, manipulated and recorded facility security surveillance systems likely will become the norm in the future.
- As sensor technology develops it will be necessary to continually upgrade those in cargo handling areas that increase the probability of detecting explosives, biological, chemical and radiation threats.
- Non-intrusive scanning devices (sniffers), imaging and pattern recognition equipment can be employed effectively at “choke points” such as under bridges, boarding ramps and cargo handling cranes and conveyor systems.
- A contracted mobile integrated security package that would meet the needs of an occasional cruise ship visit to a port or to respond to specific intelligence will need to be developed. As a minimum it would include an underwater detection and response system, an integrated radar and AIS system, an integrated portable perimeter security system and some sort of coordination capability including sufficient communications to make it all function effectively. Likely the package would include an appropriately trained workforce.
- Formalised training programs will need to be established for all personnel with duties and responsibilities under the Marine Transportation Security Act.
- General security awareness training will need to be included as mandatory requirement for all personnel to whom a port worker’s pass is issued.
- Programs for continuous improvement in security measures and equipment will need to be included as part of all acquisition programs. The reality is that “you can’t just buy it once.” Those that are intent upon violating peace, order and the process of good government are actively engaged in developing counter-measures as soon as any new system is implemented.

Follow On Work

- A detailed survey and registry of SMEs be established to track capability in the marine security sector, as no currently available database appears to satisfactorily capture this information; and
- Further definition and details of Technology Demonstrators be undertaken.

GLOSSARY OF ACRONYMS

AIS	Automatic Identification System
AUV	Autonomous Underwater Vehicle
CBSA	Canadian Border Security Agency
CCG	Canadian Coast Guard
CFSEU	Combined Forces Special Enforcement Unit
CIC	Citizenship and Immigration Canada
CRMP	Coastal Recognised Maritime Picture
CSIS	Canadian Security Intelligence Service
DFO	Department of Fisheries and Oceans
IBET	Integrated Border Enforcement Team
IMSWG	Interdepartmental Maritime Security Working Group
INSET	Integrated National Security Enforcement Team
MCTS	Marine Communications and Traffic System
MIMDEX	Marine Information Management and Data Exchange
MOC	Maritime Operations Centre
MSOC	Marine Security Operations Centre
NDCC	National Defence Command Centre
NRMP	Nationally Recognised Maritime Picture
NSIS	National Security Intelligence Section
NSP	National Security Policy
RCC	Rescue Coordination Centre
RCMP	Royal Canadian Mounted Police
RDG	Regional Director General
RMIS	Regional Marine Information System
ROV	Remotely Operated Vehicle
SAR	Search and Rescue
SITCEN	Transport Canada Situation Centre
SME	Small and Medium Enterprise
TC	Transport Canada
USA	United States of America
USCG	United States Coast Guard
VPA	Vancouver Port Authority
VTMS	Vessel Traffic Management System

Annex A Maritime Companies.xls

Company Name	Address	City	Province	Postal Code	Category	Sub-Category	Sub-Category	Product(s)	Total Sales	Exports	Employees	Ownership	Founded	Phone	Email	Website	CDIA	CFN	As Of	Remarks
A F Theriault & Son Ltd	Box 10, Meteghan River	METEGHAN RIVER	NS	B0W 2J0	Surface	Surveillance		Boat Building, Repair	?	?	?	?	?	(902)645-2327	?	http://www.aftheriault.com			CFN	
AERDE Environmental Research	P.O. Box 1002 Stn. Central	HALIFAX	NS	B3J 2X1	Command and Control	Surveillance	Training	Training in Synthetic Aperture Radar and Data Handling for RADARSAT	\$100-200K	\$1-100K	?	Canada	1987	(902) 423-2211	dwerle@fox.nstn.ca	?			4/23/2003	
Aliant Telecom Inc.	?	HALIFAX	NS	B3J2W3	Command and Control	Communications		Telephone, Internet, Communications	?	?	100 to 199	?	?	?	?	?			CFN	
All-Tech Environmental Services Limited	99 Rocky Lake Dr., Suite # 18	BEDFORD	NS	B42T3	Services	Environmental		Environmental Services	?	?	?	?	?	(902)835-3727	?	http://www.toalltech.com/lead.php			CFN	
Alliance for Marine Remote Sensing Ass.	P.O. Box 1153	HALIFAX	NS	B3J 2X1	Services	Surveillance		Remote Sensing Consulting	?	?	3	Canada	1990	(902) 491-3571	amrsadmin@waterobserver.org	http://www.waterobserver.org			9/17/2003	Non profit Association
AMIRIX Systems Inc.	77 Chain Lake Dr.	HALIFAX	NS	B35 1E1	Command and Control			Software and Hardware Development	\$1-5M	\$500-999K	50	Canada	1981	(902) 450-1700	info@amirix.com	http://www.amirix.com			1/22/2004	
Apex Industries Inc.	120 Millennium Blvd.	MONCTON	NB	E1E 2G8	Services	Security	Surface	Steel fabrication, Doors, Buoys, Shallow Draft Vessels	\$25-50M	\$25-50M	200	Canada	1961	(506) 857-1600	bgdobbin@apexindustries.com	http://www.apexindustries.com			4/3/2003	
Applied Courseware Technology Inc.	P.O. Box 20018	FREDERICTON	NB	E3B 6Y8	Services	Personnel	Training	Computer Based Training in Handling Dangerous Goods	?	?	?	Canada	?	(506) 622-5930	act@integrator.com	http://www.integrator.com			6/30/2003	
Aqua Data Atlantique	194 Wright Ave.	DARTMOUTH	NS	B3B 1R6	Services	Environment	Sensors	Water Works Analysis	\$200-500K	?	?	Canada	1996	(450) 638-6128	hugron@aquadata.com	http://aquadata.com			2/20/2003	
Atlantic Aero Marine Supply and Manufacturing Ltd.	51 Raddall Avenue, Unit #3	DARTMOUTH	NS	B2Y4B9	Personnel	Safety		Marine Safety Equipment	?	?	5 to 9	?	?	(902)481-9000	sales@atlanticaeromarine.com	?			CFN	
Bridgeport Wire Rope & Chain Ltd	70 Akerley Blvd.	DARTMOUTH	NS	B3B 1R1	Surface			Camouflage Systems	?	?	?	Canada	?	(902) 468-0300	?	http://www.bridgeportwire.com			1/28/2004	
Brooke Ocean Technology Limited	11-50 Thornhill Dr.	DARTMOUTH	NS	B3B 1S1	Underwater	Sensors		Sensor Buoys, Handling gear	\$1-5M	\$1-5M	7	Canada	1983	(902) 468-2928	sales@brooke-ocean.com	http://www.brooke-ocean.com			8/13/2003	
C-Vision Limited	21 Tantram Crescent	AMHERST	NS	B4H4S8	Command and Control			Electronics/Software Development	?	?	?	?	?	(902)667-1228	cartmill@csrep.com	www.cvision.ca			CFN	
Canadian Centre for Marine Communication	P.O. Box 8454	ST. JOHN'S	NL	A1B 3N9	Services	Command and Control	Communications	Partner in Marine Based Projects	?	?	15	Canada	1989	(709) 579-4872	info@ccmc.nf.ca	http://www.ccmc.nf.ca			4/16/2004	
Canadian Seabed Research Limited	341 Myra Rd.	PORTERS LAKE	NS	B3E 1G2	Services	Mapping	Surveillance	Surveying, Sea bed Mapping	?	?	?	Canada	1985	(902) 827-4200	csr@csr-marine.com	http://www.csr-marine.com			6/3/2003	
Canadian Universal Technologies, Ltd.	1600 Bedford Hwy, Suite 100-153	BEDFORD	NS	B4A 1E8	Command and Control	Communications		Communications Security Equipment and Components	?	?	?	?	?	(902) 830-9484	unitechs@canada.com	?			2/21/2004	
Cansel Survey Equipment (Canada) Ltd	95 Akerley Blvd	DARTMOUTH	NS	B3B1R7	Services	Mapping		Surveying	?	?	20 to 49	?	?	(902)468-3971	?	www.cansel.ca			CFN	
CARIS	115 Waggoners Lane	FREDERICTON	NB	E3B 2L4	Services	Mapping	Surveillance	Geomatics Technology	?	?	125	Canada	1979	(506) 458-8533	info@caris.com	http://www.caris.com			5/10/2004	
Centre for Cold Ocean Research Engineering	R. A. Bartlett Bldg, Morrissy Rd.	ST. JOHN'S	NL	A1B 3X5	Underwater	Services		Engineering Services	\$5-10M	\$1-5M	75	Canada	1975	(709) 737-8354	info@c-core.ca	http://www.c-core.ca			6/5/2003	
CHC Helicopter Corporation	P.O. Box 5185 Stn. C	ST. JOHN'S	NL	A1C 5V5	Services	Surveillance	Air	Non scheduled Helicopter Services	?	?	2000	Canada	?	(709) 570-0700	chcanagan@sjghns.chc.ca	http://www.chc.ca/			4/26/2004	
CKT Nova Scotia Limited	10 Second St.	BEDFORD	NS	B4A 2A1	Manufacture	Security	Environment	Advanced Container Technology and Fire Gas Detection systems	?	?	?	Canada	?	(902) 835-4531	beckerson@ns.sympatico.ca	?			4/1/2003	
Clean Harbors Canada, Inc	640 McElmorn Road	DEBERT	NS	B0M1G0	Env Sys			Environmental Services/Rescue Services	?	?	?	?	?	(902)662-3336	winters.scott@cleanharbors.com	www.cleanharbors.com			CFN	
Combustion Dynamics Ltd.	400-1888 Brunswick St.	HALIFAX	NS	B3J 3J8	Services	Command and Control		Software Development	?	?	11	Canada	1984	(902) 425-5101	march@combdyn.com	http://www.combdyn.com			1/27/2003	
Composites Atlantic Limited	P.O. Box 1150	LUNenburg	NS	B0J 2C0	Manufacture	Surface	Subsurface	Sensor Launchers and Platforms	\$10-25M	\$5-10M	125	Canada	2000	(902) 634-8448	mquilton@compositesatlantic.com	http://www.compositesatlantic.com			4/16/2004	
CompuSult Limited	P.O. Box 1000	MOUNT PEARL	NL	A1N 3C9	Services	Command and Control		Software	\$1-5M	\$200-500K	32	Canada	1985	(709) 745-7914	info@compusult.net	http://www.compusult.net			6/12/2003	
Custom Assemblies Limited	541 Ferdinand Blvd.	DIEPPE	NB	E1A 7G1	Manufacture			Electronic Component Manufacture	\$1-5M	\$100-999K	60	Canada	1985	(506) 877-0734	CEAL@customelectronic.com	http://www.customelectronic.com			9/23/2003	
Custom Fabricators & Machinists	P.O. Box 3038 Stn. "B"	SAINT JOHN	NB	E2M 4X7	Surface	Surveillance		Shallow Water Vessels	?	?	175	Canada	1968	(506) 635-5656	roger.derek@customfabricators.com	?			5/23/2003	
D & L Engineering Sales Limited	1057 Barrington Street	HALIFAX	NS	B3J2Z1	Services			Engineering/Safety Control System	?	?	20 to 49	?	?	(902)429-3790	info@dl-eng.com	http://www.dl-eng.com			CFN	
Diaphonics Inc.	313-5595 Fenwick St.	HALIFAX	NS	B3H 4M2	Personnel	Surveillance	Security	Voice Security, Voice Biometrics, Call Recording, Audio Analysis.	\$200-500K	\$200-500K	13	Canada	2000	(902) 446-3680	jeremyb@diaphonics.com	http://www.diaphonics.com			7/5/2004	
Digital Products Limited	37 Hanover St.	SAINT JOHN	NB	E2L 3G1	Command and Control	Communications		Telecommunications System Components	\$500-999K	\$1-99K	6	Canada	1974	(506) 635-0050	marketing@dpl.ca	http://www.dpl.ca			1/13/2004	
Dominion Diving Limited	7 Canal St.	DARTMOUTH	NS	B2Y 2W1	Underwater	Surveillance		ROV, Diving	?	?	125	Canada	1969	(902) 434-5120	jscott@dominiondiving.com	http://www.dominiondiving.com			2/27/2003	
DSS Marine Incorporated	152 Rocky Lake Drive	BEDFORD	NS	B4A2T6	Personnel	Safety		Marine/Military/Safety Equipment	?	?	5 to 9	?	?	(902)835-4848	?	http://www.dssmarine.com			CFN	
E.J.E. Trans-Lite Inc.	P.O. Box 427	ST. JOHN'S	NL	A1C 5K4	Personel	Search and Rescue	Surface	Diving Gear, PDF Lights	\$1-5M	\$1-5M	4	Canada	1988	(709) 747-3772	mail@ejetranslite.com	http://www.ejetranslite.com			4/15/2004	
Earth Information Technologies	1587 Dresden Row	HALIFAX	NS	B3J 2K4	Services	Command and Control		Geomatics, Computer Hardware	\$200-500K	\$1-100K	4	Canada	1989	(902) 420-1435	earth@attcanada.ca	http://eitgroup.com			4/11/2003	
Eastern Fence Erectors Limited	47 Troop Avenue	DARTMOUTH	NS	B3B2A7	Surface	Security		Fence Construction	?	?	5 to 9	?	?	(902)468-2455	?	?			CFN	
Expert Fence Co. Ltd.	P.O. Box 1183	BATHURST	NB	E2A 4H9	Surface	Security		Fencing	?	?	?	?	?	(506) 546-9804	?	?			12/1/2003	
Fibretek Inc.	P.O. Box 910 Station Central	HALIFAX	NS	B3J 2V5	Command and Control	Communications		Fibre Optics	\$5-10M	?	30	Canada	1992	(902) 832-7999	sales@fibretek.com	?			5/28/2003	
Fleetway Inc	200 - 155 Chain Lake Drive	HALIFAX	NS	B3S1B3	Services			Engineering, Logistics, Project Mgmt	?	?	10 to 19	?	?	(902)494-5700	sales@fleetway.ca	http://www.fleetway.ca			CFN	
GeoNet Technologies Inc.	P.O. Box 3989	CENTRAL BEDEQUE	PE	C0B 1G0	Services	Command and Control		Digital Mapping and Surveying	\$500-999K	?	15	Canada	1994	(902) 887-3170	mike.pearson@geonet-tech.com	http://www.geonet-tech.com			1/21/2003	
Geospectrum Technologies Inc.	30 Bel Ayr Ave.	DARTMOUTH	NS	B2V 2E1	Underwater	Sensors		Acoustic Transducers	?	?	1	Canada	1994	(902) 434-3906	barstrong@geospectrum.ca	http://www.geospectrum.ca			5/27/2003	
Guigne International Limited	695 St. Thomas Line	PARADISE	NL	A1L 3V2	Underwater	Surveillance	Sensors	Acoustic Sensors, Specialized Sensors, Space(NASA) Experiments	?	?	50	Canada	1989	(709) 895-3819	gill@guigne.com	http://www.guigne.com			1/30/2004	
Helical Systems	One Research Drive	DARTMOUTH	NS	B2Y4M9	Services	Command and Control		Software/Satellite Imaging	?	?	?	?	?	(902)429-1785	info@helical.ns.ca	http://www.helical.ns.ca			CFN	
Hyperspectral Data International Inc	119-7071 Bayers Rd.	HALIFAX	NS	B3L 2C2	Subsurface	Surface	Sensors	Airborne Hyperspectral Imager, Data Analysis	?	?	?	Canada	1997	(902) 461-2161	hdinfo@hdi.ns.ca	http://www.hdi.ns.ca			4/30/2004	
Ibridge Inc.	480 Main St.	WOODSTOCK	NB	E7M 2C1	Command and Control	Surveillance		Software, Information Management and Control Systems	\$1-5M	\$500-999K	10	Canada	1995	(506) 328-4282	ibridge@ibridge.net	?			5/10/2004	
IMP Group International Inc.	2651 Joseph Howe Dr.	HALIFAX	NS	B3L 4T1	Manufacture	Surface	Subsurface	Aerospace Systems, Electronics, Marine Products	?	?	2750	Canada	1967	(902) 453-2400	webmaster@impgroup.com	http://www.impgroup.com			5/30/2003	
IMP Group Limited (Marine Division)	P.O. Box 8560	ST. JOHN'S	NL	A1B 3P4	Underwater	Surveillance	Surface	Buoys, Search and Rescue Equipment	?	?	46	Canada	?	(709) 722-4221	imp.marine@impgroup.com	http://www.impgroup.com/			4/19/2004	
Instrumar Limited	P.O. Box 13246 Stn. A	ST. JOHN'S	NL	A1B 4A5	Environment	Surveillance	Sensors	Award Winning Specialized Sensors	\$1-5M	\$500-999K	40	Canada	1980	(709) 726-8460	info@instrumar.com	http://www.instrumar.com			11/18/2002	
Instrument Concepts - Sensor Software Inc.	P.O. Box 206	DEBERT	NS	B0M 1G0	Underwater	Sensors		Acoustic Navigation and Instrumentation	\$200-500K	\$200-500K	4	Canada	1988	(902) 641-3000	info@canada@instrumentconcepts.com	http://www.InstrumentConcepts.com			6/4/2004	Located at UNB
Interactive Visualization Systems Inc.	P.O. Box 69000	FREDERICTON	NB	E3B 6C2	Services	Command and Control		3D Software	\$500-999K	\$500-999K	10	Canada	1994	(506) 454-4487	ivs@ivs3d.com	http://www.ivs3d.com			1/30/2004	
Internav Ltd.	P.O. Box 1261 Stn A	SYDNEY	NS	B1P 6J9	Manufacture	Surface	Subsurface	Navigation Systems, Distress Communications Simulators	\$500-999K	\$200-500K	16	Canada	1976	(902) 564-2043	john.currie@ns.sympatico.ca	http://www.internav.ca			5/11/2004	
Irving Shipbuilding Inc.	P.O. Box 9100	HALIFAX	NS	B3K 5M7	Surface	Subsurface		Vessel Design and Manufacture	?	?	1000	Canada	?	(902) 423-9271	marketing@irvingshipbuilding.com	http://www.irvingshipbuilding.com			8/6/2004	
LearnStream Inc.	414 York St.	FREDERICTON	NB	E3B 3P7	Services	Training		Courseware Design	?	?	170	Canada	1993	(506) 447-4900	info@learnstream.com	http://www.learnstream.com			3/3/2003	
Logical Paths Training Development, Inc	201 Brownlow Avenue	BEDFORD	NS	B4A1E8	Personnel	Training		Training	?	?	1 to 4	?	?	(902)468-7246	No website	?			CFN	
Lunenburg Industrial Foundry & Engineering Ltd.	P.O. Box 1240	LUNenburg	NS	B0J 2C0	Surface	Surveillance	Underwater	Boats, Buoys	\$1-5M	\$200-500K	60	Canada	1891	(902) 634-8827	mail@lunenburgfoundry.com	http://www.lunenburgfoundry.com			4/20/2004	
MacDonald Dettwiler and Associates	60-1000 Windmill Rd.	DARTMOUTH	NS	B3B 1L7	Underwater	Command and Control		Acoustic Sensors, Display Systems	\$10-25M	?	60	Canada	1986	(902) 481-4392	?	http://halifax.mda.ca			7/31/2003	
MacDonnell Group	1505 Barrington St., Suite 1100	HALIFAX	NS	B3J2Z1	Services			Consulting, Engineering, Environmental	?	?	20 to 49	?	?	(902)425-3980	ralston@mgnet.ca	http://www.mgnet.ca			CFN	
Magneto-Inductive Systems Limited	610 Myers Pt Rd	HEAD OF JEDDORE	NS	B0J 1P0	Underwater	Surveillance	Surface	Sensors, Communications	?	?	12	Canada	1989	(902) 889-2247	wrathall@magnetoinductive.com	http://www.mi-systems.com			6/17/2003	
Malley Industries Inc.	212 Halifax St	MONCTON	NB	E1C 9S2	Emergency Response	Surface	Environment	Emergency Vehicles, Mobile Command Posts	\$1-5M	\$100-200K	30	Canada	1979	(506) 859-8591	gatekeeper@malleyindustries.com	http://www.malleyindustries.com			3/18/2003	
Martec Limited	1888 Brunswick Street, Ste 400	HALIFAX	NS	B3J3J8	Services			Software Dev, Ocean Science	?	?	50 to 99	?	?	(902)425-5101	?	http://www.martec.com			CFN	
Metocean Data Systems Limited	21 Thornhill Dr.	DARTMOUTH	NS	B3B 1R9	Underwater	Surveillance	Surface	Sensor Buoys, Vessel Tracking, Search and Rescue	\$5-10M	\$1-5M	28	Canada	1985	(902) 468-2505	sales@metocean.ns.ca	http://www.metocean.com				

Annex A BC Companies1.xls

Company Name	Address	City	Province	Postal Code	Category	Sub-Category	Sub-Category	Product(s)	Total Sales	Exports	Employees	Ownership	Founded	Phone	Email	Website	CDIA	CFN	As Of	Remarks
A.G.O. Environmental Electronics Ltd.	10-626 Esquimalt Rd.	VICTORIA	BC	V9A 3L4	Underwater	Acoustic	Video	Sub Sea Video Systems, Components for Oceanographic Research	\$200-500K	\$100-200K	6	Canada	1986	(250) 396-4015	info@agenvironmental.com	http://www.agenvironmental.com			2/15/2004	Affiliated - Jasco Research Ltd. (Victoria);
Absolute Software Corp.	800-111 Dunsmair St.	VANCOUVER	BC	V6B 6A3	Command and Control	Software	Video	Computer Security	?	?	80	Canada	1993	(604) 730-9851	info@absolute.com	http://www.absolute.com			2/20/2004	
Abucco Technologies Inc	2615 Clarke St	SURREY	BC	V3H 1Z4	Surface	Security	Access Control	Wireless, smart card	?	?	?	Canada	1993	(604) 936-3600	jaro@abucco.com	http://www.abucco.com				
ACR Systems Inc.	210 - 12960 - 84th Ave.	SURREY	BC	V3W 1K7	Surface	Surveillance		Sensors and Data Loggers	\$5-10M	\$5-10M	30	Canada	1983	(604) 591-1128	enquiry@acrsystems.com	http://www.acrsystems.com			2/2/2004	
Advanced Subsea Services Ltd	8626-B Lochside Dr	Sidney	BC	V8L 1M7	Underwater	diving and ROV services		advanced diving and ROV services on call	?	?	?	Canada	?	(250) 656-2682	murray@advancedsubsea.com	http://advancedsubsea.com				
ALS Canada Ltd.	1988 Triumph St.	VANCOUVER	BC	V5L 1K5	Services	Environment	Consulting	Chemical Testing and Environmental consulting	\$5-10M	?	100	Canada	1982	(604) 253-4188	vancouver@alsenviro.com	http://www.alsenviro.com			2/27/2003	
Applied Microsystems Limited	2071 Malvern Ave.	SIDNEY	BC	V8L 5X6	Underwater	Sensors	Oceanographic Research	Geophysical Research Instruments	\$1-5M	\$1-5M	24	Canada	1974	(250) 656-0771	info@appliedmicrosystems.com	http://www.appliedmicrosystems.com			4/26/2004	
Applied Microsystems Limited	2071 Malvern Ave.	SIDNEY	BC	V8L 5X6	Underwater	Sensors		Oceanographic Sensors	\$1-5M	\$1-5M	24	Canada	1974	(250) 656-0771	info@appliedmicrosystems.com	http://www.appliedmicrosystems.com			4/26/2004	
Aqua-Guard Spill Response Inc.	100 - 1055 - 14th St.	NORTH VANCOUVER	BC	V7P 3P2	Services	Environment		Oil Spill Response Products	\$1-5M	\$1-5M	12	Canada	1992	(604) 980-4889	rick@aquaguard.com	http://www.aquaguard.com			5/23/2003	
Argon Security Technologies Inc	2922A Spring St	Port Moody	BC	V3H 1Z7	Surface	Security	Access Control	Mobile wireless surveillance and Digital Video Recorder	?	?	?	Canada	?	(604) 461-0905	info@argonsecurity.com	http://www.argonsecurity.com			Oc-02	
ASL Environmental Sciences	1986 Mills Rd	Sidney	BC	V8L 5Y3	Underwater	water measuring		water profile meters	?	?	?	Canada	?	(250) 656-2162	dileon@aslenv.com	http://www.aslenv.com				
ASL Environmental Sciences Inc	1986 Mills Rd.	SIDNEY	BC	V8L 5Y3	Underwater	Acoustic	Oceanographic Research	Environmental Sensors, Modeling	\$1-5M	\$1-5M	28	Canada	1977	(250) 656-0177	asl@aslenv.com	http://www.aslenv.com/			3/21/2003	
Axys Environmental Consulting Ltd.	2645 Mills Rd.	SIDNEY	BC	V8L 5X2	Underwater	Environment		Environmental Consulting, Weather/Wave Buoys, Weather Logging	\$1-5M	?	35	Canada	?	(250) 656-0881	consulting@axys.com	http://www.axys.com			2/19/2003	
Bonica Precision (Canada) Inc.	110-12171 Horseshoe Way	RICHMOND	BC	V7A 4V4	Underwater	Equipment		Underwater Cameras and Diving Equipment	\$1-5M	\$1-5M	19	Canada	1985	(604) 270-0812	bonica@direct.ca	http://www.bonicateam.com			4/28/2004	
Braintech Inc.	102 - 930 - 1st St W	NORTH VANCOUVER	BC	V7P 3N4	Surface	Software		Vision Guide Robotics	?	?	?	Canada	?	(604) 988-6440	info@braintech.com	http://www.braintech.com			2/6/2004	
Candian Submarine Technologies Inc	2397 King George Hwy	SURREY	BC	V4A 9N3	Underwater	Manned Submersibles			?	?	?	Canada	?	(604) 535-1657	dick@canadiansub.com	http://www.canadiansub.com				
Camnanah Technologies Inc.	Bldg 4-203 Harbour Rd.	VICTORIA	BC	V9A 3S2	Surface	Lighting		Solar Powered LED Lighting Systems	\$1-5M	\$500-999K	12	Canada	1989	(250) 380-0052	info@camnanah.com	http://www.camnanah.com			7/29/2003	
Cartel Communications Systems Inc	9415-202 St	Langley	BC	V1M 4B5	Services	Communications		Customized Wireless, dispatch communications	?	?	?	Canada	?	(604) 888-9711	doug@cartelsys.com	http://www.cartelsys.com				
Cavendish Analytical Laboratory Ltd.	1650 Pandora St.	VANCOUVER	BC	V6L 1L6	Services	Environment	Consulting	Chemical Testing and Environmental consulting	\$500-999K	?	?	Canada	1988	(604) 251-4458	cavendish@portals.ca	http://www.cavendish.ca			1/31/2003	
Cavio Corporation	21 Water St., 5th Floor	VANCOUVER	BC	V6B 1Y1	People	Surveillance		Authentication/Identification via Biometrics and Fingerprint Scan	?	?	?	Canada	?	(604) 696-0633	pmann@cavio.com	http://www.cavio.com			1/23/2003	
Code Three Emergency Vehicles Inc.	3-1660 Powick Rd.	KELOWNA	BC	V1X 7G5	Emergency Response	Vehicles	Command and Control	Emergency Vehicles, Mobile Command Posts	?	?	?	Canada	?	(250) 861-9000	codeth3@silkn.net	?		12/13/2002		
ComNav Marine Ltd	15-13511 Crestwood Place	Richmond	BC	V6V 2G1	Surface	Navigation and Guidance Systems		Shipboard Electronics	?	?	?	Canada	1983	(604) 207-1600	comnav@comnav.com	http://www.comnav.com			10/2/2003	
Computrol Security Systems Ltd.	6-7541 Conway Ave.	BURNABY	BC	V5E 2P7	People	Surveillance		Access Control Systems	\$1-5M	\$500-999K	22	Canada	1980	(604) 454-1000	?	http://www.computrol-security.com			10/18/2002	
Continental Steel Ltd.	251 Schoolhouse St.	COQUITLAM	BC	V3C 6N2	Surface	Security	Fencing	Fencing	\$1-5M	\$1-5M	12	Canada	1983	(604) 525-2673	info@cysys.net	http://www.cysys.net			5/28/2004	
Cybernetics Systems Inc.	22-1151 Horseshoe Way	RICHMOND	BC	V7A 4A5	Surface	Surveillance	Video	Video Surveillance Systems	\$1-5M	\$1-5M	77	Canada	1983	(604) 448-8829	info@cysys.net	http://www.cysys.net			5/28/2004	
DBC Marine Safety Systems Ltd.	101-3760 Jacobs Rd.	RICHMOND	BC	V6V 1Y6	Surface	Vehicles	Rescue	Boats - Inflatables and Ribs	\$5-9M	\$1-5M	7	Canada	1977	(604) 278-3221	sales@dbmarine.com	http://www.dbmarine.com			2/18/2003	
Delta Aerial Surveys Ltd.	2121-11871 Horseshoe Way	RICHMOND	BC	V7A 4V4	Services	Mapping		Digital Mapping	\$1-5M	?	?	Canada	1981	(604) 275-3505	mail@deltamap.com	http://www.deltamap.com			4/11/2004	Division of Dunlop-Beaufort
Dewey McMillin & Associates Ltd.	100-1741 Feltham Rd	VICTORIA	BC	V8N 2A4	Command and Control	Emergency Response/Explosives		Air Blast and Eblast Explosion Prediction Systems	?	?	?	Canada	1988	(250) 477-5849	dewey@blastanalysis.com	http://www.blastanalysis.com			5/27/2003	
DIVELINK Underwater Communications	14-831 Devonshire Rd	VICTORIA	BC	V9A 4T5	Underwater	Communications		Diving and Underwater Communications Systems	\$1-5M	\$200-500K	15	Canada	1990	(250) 479-4868	sales@divelink.net	http://www.divelink.net			5/19/2004	
Dynavar Networking, Inc.	207-475 Howe St.	VANCOUVER	BC	V6C 2B3	Command and Control	Communications		Voice Switching	\$25-50M	\$10-25M	75	Canada	1994	(604) 664-7457	nbell@dynavar.com	http://www.dynavar.com			3/21/2004	
Eagle Mapping Limited	201-2071 Kingsway Ave.	PORT COQUITLAM	BC	V3C 6N2	Services	Mapping		Aerial Surveying and Mapping	\$500-999K	\$200-500K	15	Canada	1985	(604) 942-5551	info@eaglemapping.com	http://www.eaglemapping.com			2/24/2003	
Electro Systems Inc.	8-415 Durand St.	VICTORIA	BC	V8T 5G8	Surface	Security	Environment	Lights, Gas Detection Systems	\$200-500K	\$1-100K	3	Canada	1969	(250) 395-0911	info@es-web.com	http://www.es-web.com			6/4/2003	
Elros Aluminium & Ironcraft Ltd.	12333 Winram Rd.	SURREY	BC	V5A 3C2	Surface	Security	Fencing	Fencing, Gates, metal- Posts	?	?	?	Canada	?	(604) 580-3332	?					
Extreme CCTV Inc	3021 Underhill Ave	Burnaby	BC	V5A 3C2	Services	Surveillance	Cameras	Infrared Illumination & Night Vision Cameras	?	?	?	Canada	?	(604) 420-7711	Jgin@ExtremeCCTV.com	http://www.ExtremeCCTV.com				
Foreshore Technologies Incorporated	118 Garden Ave.	NORTH VANCOUVER	BC	V7P 3H2	Underwater	Vehicle	Search and Rescue	Towed Diver Operated Vehicle (DOV)	?	?	?	Canada	1984	(604) 983-3111	fit@foreshore.ca	http://www.foreshore.ca			2/7/2004	
Frontier Fencing Ltd.	PO Box 2027 Stn. Main	DAWSON CREEK	BC	V8Z 6N6	Surface	Security	Fencing	Fencing	?	?	?	Canada	?	(250) 782-7773	?					
Frozen Dirt Media Corp	101-4226 Commerce Cir.	VICTORIA	BC	V8Z 6N6	Command and Control	Software		Security Software for Police and Defense.	?	?	?	Canada	?	(250) 479-1595	info@frozendirt.com	http://www.frozendirt.com			4/27/2004	
G.A. Borstad Associates Ltd.	9605 West Saanich Rd.	NORTH SAANICH	BC	V8L 5Y8	Services	Mapping		Remote Sensor Mapping	\$500-999K	\$500-999K	10	Canada	1983	(250) 656-5633	gary@borstad.com	http://www.borstad.com			2/20/2003	
GeoInfo Solutions Ltd.	10352 Arbutus Close	SIDNEY	BC	V8L 4S2	Services	Environment		Environmental Consulting, Contingency Planning, Risk Assessment	\$200-500K	?	?	Canada	1992	(250) 656-3056	bjudson@geoinfosolutions.com	http://www.geoinfosolutions.com			6/24/2003	
IDELIX Software Inc	555-1122 Mainland St	Vancouver	BC	V6B 5L1	Command and Control	Software		Pliable Focal Lens for image enhancement	?	?	?	Canada	?	(604) 656-6304	kippl@idelix.com	http://www.idelix.com				
Imagenex Technology Corp	909-1875 Broadway St	PORT COQUITLAM	BC	V3C 4Z1	Underwater	Sonars	digital processing	HiF Freq sonars for ROVs, Sidescan, Bottom Profile etc	?	?	?	Canada	?	(604) 944-8248	imagenex@npsnet.com	http://www.imagenex.com			13/4/2004	
Imagenex Technology Corp.	209-1875 Broadway St.	PORT COQUITLAM	BC	V3C 4Z1	Underwater	Acoustic	Software	Colour Image Sonar Systems and S/W, Radar	?	?	?	Canada	1989	(604) 944-8248	imagenex@npsnet.com	http://www.imagenex.com				
Imagis Technologies Inc.	1630-1075 Georgia St. W.	VANCOUVER	BC	V6E 3C9	People	Surveillance		Facial Recognition Software	\$1-5M	\$1-5M	20	Canada	1990	(604) 684-2449	info@imagistechnologies.com	http://www.imagistechnologies.com			6/19/2003	
Interactive Oil Spill Training Center	602-2222 Bellevue Ave.	WEST VANCOUVER	BC	V7V 1C7	Services	Environment		Oil Spill Response Training - E-learning	?	?	?	Canada	1991	(604) 922-4522	hrabin@iostc.com	http://www.iostc.com			1/8/2004	
International Hydro Cut Tech Corp.	207-11806 Welsh St.	NORTH VANCOUVER	BC	V7P 1B3	Emergency Response	Vehicles		Tactical Breaching Equipment and Bomb Disruptors	\$1-5M	\$555-999K	14	Canada	1988	(604) 980-1415	info@hydrocut.com	http://www.hydrocut.com			5/10/2004	
International Venturecraft Corp.	6200 McKay Ave.	BURNABY	BC	V5H 4M9	Underwater	Vehicles		Manned Submersibles	?	?	?	Canada	1987	(604) 436-5653	info@ivccorp.com	http://www.ivccorp.com			5/10/2003	
Inukton Services Ltd.	C-2568 Kenworth Rd.	NANAIMO	BC	V9T 3M4	Underwater	Vehicle	Surface	ROV, Robotics, Underwater Cameras, EOD	\$1-5M	\$1-5M	25	Canada	1989	(250) 729-8080	inukton@inukton.com	http://www.inukton.com			1/27/2004	
ISE Research Ltd.	1734 Broadway St.	PORT COQUITLAM	BC	V3C 2M8	Underwater	Vehicle		Autonomous Underwater Vehicle (AUV)	?	?	?	Canada	1982	(604) 942-5223	iser@ise.bc.ca	http://www.ise.bc.ca			7/16/2004	
JASCO Research Ltd	2101-4464 Markham St	Victoria	BC	V8Z 7X8	Underwater	Acoustics	Oceanography	acoustic and image analysis	?	?	?	Canada	?	(250) 483-3300	rob@jasco.com	http://jasco.com				
Kamiloops Wire Products (1983) Ltd.	3299 Westsyde Rd.	KAMLOOPS	BC	V6P 6T7	Surface	Security	Fencing	Fencing, Gates	\$500-999K	\$200-500K	8	Canada	1991	(604) 267-7800	guy@kinetic.ca	http://www.kinetic.ca			5/28/2003	
Kinetic Sciences Inc.	500-655 Kent Ave. North W.	VANCOUVER	BC	V6P 6T7	People	Surveillance		Finger Print Detection	?	?	?	Canada	?	(604) 689-7117	peter@kineticsystems.com	http://www.kineticsystems.com			12/9/2003	
Klein Systems Group Ltd.	300-1901 Rosser Ave	BURNABY	BC	V5C 6R6	Command and Control	Software		Vessel Traffic, Harbour Operations, Pilotage Management Systems	?	?	?	Canada	?	(604) 689-7117	info@kleinsystems.com	http://www.kleinsystems.com				
Kongsberg Simrad Mesotech Ltd.	1598 Kabet Way	PORT COQUITLAM	BC	V3C 5M5	Underwater	Acoustic	Surveillance	Sonar and Echo Sounding Equipment, Under Water Surveillance Equipm	\$10-25M	\$10-25M	50	Canada	1972	(604) 464-8144	vancouver.sales@kongsberg-simrad.com	http://www.kongsberg-simrad.com			2/7/2002	
MacDonald, Dettwiler and Associates Ltd.	13800 Commerce Pky.	RICHMOND	BC	V6V 2J3	Command and Control	Sensors	Surveillance	System Integrators and Designers, Various	\$50M-plus	?	2200	Canada	1969	(604) 278-3411	info@mda.ca	http://www.mda.ca/			3/23/2004	
Mustang Survival Corp.	3810 Jacobs Rd.	RICHMOND	BC	V6V 1Y6	Services	Personnel Safety		Personnel Water Safety Gear	?	?	?	Canada	?	(604) 270-8631	mustang@mustangsurvival.com	http://www.mustangsurvival.com			5/2/2003	
Northern Airborne Technology Ltd.	1925 Kirschner Rd.	KELOWNA	BC	V1Y 4N7	Surface	Communications		Radios, PA Systems, Sirens	\$5-10M	\$5-10M	75	Canada	1979	(250) 763-2232	general@natech.com	http://www.northernairborne.com			2/10/2003	
OceanWorks International Corporation	3-1225 E. Keith Rd.	NORTH VANCOUVER	BC	V7J 1J3	Underwater	Vehicle	Diving	ROV, Handsull, Deep Diving Rescue Apparatus	?	\$10-25M	49	Canada	1986	(604) 896-5800	info@oceanworks.cc	http://www.oceanworks.cc			6/2/2003	
Offshore Systems International Ltd	107-930 West 1st St	North Vancouver	BC	V7P 3N4	Command & Control	Picture Compilation		COP IDS, ECPINS	?	?	?	Canada	?	(604) 904-4690	andrew.came@osicorp.com	http://www.osicorp.com				
Orcatron Communications Ltd.	4775 Granville St.	VANCOUVER	BC	V6H 3M2	Underwater	Communications	Diving	Underwater Wireless Communications Systems	\$1-5M	\$1-5M	8	Canada	1983	(604) 941-7909	orcatron@tel					

Annex B – Potential Investigation Areas for SMEs

Category	Activity	Background Paragraph(s)
Sensors and Detectors	<ul style="list-style-type: none"> • Container monitoring (Smart Containers) • Remotely Operated Vehicles • Remote imaging capability • Underwater scanners (fixed and mobile) • Autonomous Underwater Vehicles • Uninhabited Air Vehicles • Automatic Identification Systems • Biometric Identification Systems • Automated Alarm and Alerting Systems 	<ul style="list-style-type: none"> • 49,54 • 59,73,79 • 59,71,77,82 • 59,71,77,82 • 73,79 • 69 • 59,69 • 18,39,47 • 54,88
Information Management	<ul style="list-style-type: none"> • Database Management • Data Exchange Protocols • Integration and Display Technology • Port Coordination Centres and Facilities 	<ul style="list-style-type: none"> • 31,81 • 28,56-58,61,62 • 61,67,84 • 18,19,27,77
Security Services	<ul style="list-style-type: none"> • Developing Security Plans • Security Assessments • Security Clearances • Mobile Security Teams • Harbour Patrol • Facility augmentation personnel for increased MARSEC levels • Diving Inspection Teams • Exercise Definition, Planning and Implementation • Design and Control of Access Authorisation Tools 	<ul style="list-style-type: none"> • 3,21,34-36,51 • 45 • 54 • 92 • 86 • 4,88,90 • 53,59,81 • 63 • 18,39,47,54
Training	<ul style="list-style-type: none"> • Observation and Reporting Techniques • Patrol Techniques • Boat Handling • Understanding and Implementing Regulations • Provision of educational tools, such as distance learning and compliance monitoring • Crisis Management and Decision-making techniques and training 	<ul style="list-style-type: none"> • 60 • 88 • 3 • 45,63
Communications	<ul style="list-style-type: none"> • Secure communications equipment 	<ul style="list-style-type: none"> • 18,61

<p>Technology Demonstration Projects</p>	<ul style="list-style-type: none"> • Ship bottom monitoring at anchorage or when entering a port. An upward looking high frequency sonar integrated with a video capability and monitored real time in the Port Coordination Centre • Coastal surveillance in an area currently devoid of capability other than a capability to receive voluntary voice reports. Integrate an AIS and portable radar into the voice transmission system to provide for inclusion in the NRMP • Cruise ship or high threat facility in a regional port. Securing a cruise ship terminal against threats from all threat vectors, particularly underwater and from the land perimeter. • Cruise ship terminal in an occasional port. A mobile capability that can provide for security of a cruise ship berth for the duration of a visit. • A fixed and deployable sensors and response capability that can begin to address the underwater threat. In order to demonstrate real capability it will be necessary to have additional surface movement sensors integrated with the underwater sensors. As a package they will require to be monitored in real time from the port coordination centre. • Using an AIS and radar system demonstrate their utility in acting as a port vessel traffic management system where one is not currently available. 	<ul style="list-style-type: none"> • 53,59,77,82 • 46,50,51,61,68,69 • 53,83,88 • 54,92,93 • 59,82 • 21,84,85
--	---	---

Catégorie	Activité	Paragraphe(s)
Capteurs et détecteurs	<ul style="list-style-type: none"> • Surveillance des conteneurs (conteneurs intelligents) • Engins télécommandés • Imagerie télécommandée • Scanneurs sous-marins (fixes et mobiles) • Véhicules sous-marins autonomes • Véhicules aériens sans équipage • Systèmes d’identification automatiques • Systèmes d’identification biométriques • Systèmes d’alarme et d’alerte automatiques 	<ul style="list-style-type: none"> • 49,54 • 59,73,79 • 59,71,77,82 • 59,71,77,82 • 73,79 • 69 • 59,69 • 18,39,47 • 54,88
Gestion de l’information	<ul style="list-style-type: none"> • Gestion de bases de données • Protocoles d’échange de données • Technologie d’intégration et d’affichage • Centres et installations de coordination portuaire 	<ul style="list-style-type: none"> • 31,81 • 28,56-58,61,62 • 61,67,84 • 18,19,27,77
Services de sécurité	<ul style="list-style-type: none"> • Élaboration de plans de sécurité • Évaluations de sécurité • Attestations de sécurité • Équipes mobiles de sécurité • Patrouilles portuaires • Personnel de renfort pour niveaux d’alerte de sécurité accrue • Équipes de plongeurs-inspecteurs • Définition, planification et mise en oeuvre d’exercices • Conception et contrôle d’instruments d’autorisation d’accès 	<ul style="list-style-type: none"> • 3,21,34-36,51 • 45 • 54 • 92 • 86 • 4,88,90 • 53,59,81 • 63 • 18,39,47,54
Formation	<ul style="list-style-type: none"> • Techniques d’observation et de comptes rendus • Techniques de patrouille • Pilotage d’embarcation • Connaissance et mise en application de règlements • Outils éducatifs tels l’apprentissage à distance et le contrôle d’observation • Techniques et formation de gestion de crise et prise de décisions 	<ul style="list-style-type: none"> • 60 • 88 • 3 • 45,63
Communications	<ul style="list-style-type: none"> • Systèmes de communication protégés 	<ul style="list-style-type: none"> • 18,61

<p>Projets de démonstration technologique</p>	<ul style="list-style-type: none"> • Observation de coques de navire au mouillage ou à l'entrée du port. Sonar haute fréquence à vision vers le haut intégré à un système vidéo et fonctionnant en temps réel au centre de coordination portuaire • Surveillance côtière dans un secteur doté uniquement d'une capacité de recevoir des comptes rendus verbaux volontaires. Intégrer un SIA et un radar portatif au système de transmission vocal pour l'inclure dans le NRMP • Terminal de navires de croisière ou installations à risque élevé dans un port régional. Protéger un terminal de navires de croisière contre tous les types de menaces, et particulièrement les menaces sous-marines et les menaces des zones terrestres adjacentes. • Navires de croisière dans un port de circonstance. Ressources mobiles pouvant assurer la sécurité à un poste de navire de croisière pendant la durée de l'escale. • Capteurs fixes et déployables et ressources d'intervention pour résoudre le problème de la menace sous-marine. Pour démontrer une capacité véritable, il faudra intégrer aux capteurs sous-marins des capteurs de mouvement de surface. Il faudra pouvoir surveiller l'ensemble du système en temps réel à partir du centre de coordination portuaire. • Démontrer l'utilité d'un SIA combiné à un système radar comme système de gestion de la circulation portuaire dans un endroit où il n'y a pas de tel système. 	<ul style="list-style-type: none"> • 53,59,77,82 • 46,50,51,61,68,69 • 53,83,88 • 54,92,93 • 59,82 • 21,84,85
---	---	---